PROTECTING PRIVACY WHEN USING TELEHEALTH TECHNOLOGY IN HEALTHCARE

Volume 1 – Issues and Recommendations

Telehealth Deployment Research Testbed

Grant Award # 1 D1BTM 0005-01

October 2002

Prepared for:
US Department of Health and Human Services
Office for the Advancement of Telehealth
5600 Fishers Lane, Room 11A-55
Rockville, MD 20857

Prepared by:
Advanced Technology Institute
5300 International Blvd.
North Charleston SC 29418

Authors

This report was created through the joint efforts and contributions of a number of individuals. Lynn Crane was the coordinator and principal writer. Nina Antoniotti and Sam Burgiss provided significant input to development of telemedicine/telehealth background materials and to all authors' overall understanding of the particular constraints and challenges faced in telehealth. Chuck Doarn provided technical observations and recommendations on telehealth's use and potential vulnerabilities of certain technologies, and Alan Goldberg contributed the report's policy observations. Archie Andrews and Jack Corley provided significant contributions to our research and presentation of issues and recommendations.

Lynn Crane, MBA *Principal Author*
Advanced Technology Institute
North Charleston, SC

Archie D. Andrews, MS
Advanced Technology Institute

Jack Corley, MS
Advanced Technology Institute

Nina M. Antoniotti, RN, MBA, PhD
Marshfield, WI

Samuel G. Burgiss, PhD
Knoxville, TN

Charles R. Doarn, MBA
Richmond, VA

Alan S. Goldberg, JD, LLM
Goulston & Storrs, Washington, DC

The authors would like to thank the individuals listed below for their assistance in developing this report.

Contributors

Key contributors provided policy and technical expertise for the report. Anna Spencer, JD, and Robert J. Waters, JD, of Arent Fox provided an assessment of the effect of current and proposed regulations on telehealth activities. Johnathan Coleman, Stephen Pellissier, MS, Jack Stinson, ME, PhD, and Scott West, MS, of the Advanced Technology Institute provided information protection expertise for the report's technology recommendations.

Acknowledgements

Individuals who assisted report development by reviewing issues and vulnerabilities identified in this research and providing input on their relative importance in the practice of telemedicine and telehealth include: David Balch, MA; Alan Branigan; Keith Duerr; John P. Fanning, LLB; Stewart Ferguson, PhD; Carol B. Haberman, MS, MPA; Joanne Kumekawa, MBA; Dena Puskin, ScD; Max E. Stachura, MD; and Lydia Weisser, DO. Sarah Hartline and Skip Crane, MBA, of ATI made other important contributions to content and development of the report.

Source of Funding for the Study

This report was prepared as part of the Telehealth Deployment Research Testbed (TDRT) established by the Office for the Advancement of Telehealth (OAT). The study was funded through OAT, the Health Resources and Services Administration (HRSA), and the Office of the Assistant Secretary for Planning and Evaluation (OASPE) of the U.S. Department of Health and Human Services.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

Executive Summary

This report documents the observations and recommendations resulting from a study of the privacy, confidentiality, and security issues unique to delivery of care through telehealth interactions. The study focused on privacy protection in two types of telehealth[1]—its telemedicine[2] care delivery component, and its use of the Internet for care delivery and patient/consumer education. It is important to note that use of electronic tools in traditional in-person care is growing as the tools become more generally available on clinicians' desktops—"Many physicians use telemedicine without realizing it, since telemedicine can be a telephone consult, interpreting a diagnostic test from a distance, transmitting medical information across state lines, or monitoring a patient across national boundaries."[3]

Because telemedicine/telehealth participants do not meet in person as in traditional care, information and communications technologies such as interactive videoconferencing, electronic messaging, and web interaction are employed to simulate the types of interaction that typically occur in an in-person setting. The use of these electronic techniques is the primary difference between telehealth and traditional in-person care delivery and, therefore, the basis for most telehealth-unique information protection issues. Experts in the fields of telehealth practice and technology, privacy policy, and information protection technologies performed this investigation and developed the study's recommendations for improving the level of protection afforded to private patient information when care is delivered through telehealth and telemedicine.

Information Privacy Regulations

Extensive federal and state regulations, regulations generated by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO),[4] and guidance issued by numerous healthcare professional organizations require that patient information be protected. Beyond that, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) legislation enacted by Congress[5] requires implementation of various mechanisms for ensuring privacy of healthcare information. HIPAA regulations relevant to protecting patient information include the Privacy Standards[6] (which were finalized on August 14, 2002) and the Security Standards[7] (which are in Notice of Proposed Rule Making status as of this writing). The Privacy Standards

[1] The full text of one definition of telehealth is, "the use of modern information and telecommunication technologies to provide health care services and access to health information for health professionals and consumers to train and educate health professionals; to increase awareness and educate the public about health-related issues; and to facilitate research about health care issues across a distance." From Puskin, Mintzer, & Wasem (1997, p. 276).

[2] One definition of "telemedicine," and there are many, is "a subset of telehealth, allowing a clinician to provide care via telecommunications." Chaffee (1999).

[3] Ferri & Klein (2000).

[4] JCAHO, the Joint Commission on Accreditation of Healthcare Organizations, provides "health care accreditation and related services that support performance improvement in health care organizations." See "Who Is."

[5] Appendix A provides a brief overview of HIPAA.

[6] Standards for Privacy of Individually Identifiable Health Information (2000). Published in the Federal Register on December 28, 2000 (with Final Modifications published on August 14, 2002), the Privacy Standards require compliance by April 14, 2003 (April 14, 2004, for small health plans). 45 CFR § 164.530(c)(1). Available at: http://www.hhs.gov/ocr/hipaa/finalreg.html .

[7] Security and Electronic Signature Standards (Proposed Rule) (1998). The proposed Security Standard outlines requirements for administrative procedures, physical safeguards, technical security services and technical security mechanisms for guarding data integrity confidentiality, and availability. 45 CFR § 142.308. Available at: http://aspe.hhs.gov/admnsimp/nprm/seclist.htm.

require protection of health information that is created or maintained by covered entities,[8] regardless of the form in which it is used—on paper, electronically, and verbally, calling for use of "…appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The Security Standards, applicable to the same organizations as the Privacy Standards, set guidelines for developing and maintaining the security of all electronic individual health information.

Issues

The core observation of this study is that a healthcare organization's operational practices and information protection capabilities characterize and sustain its information privacy culture. Failure to maintain a balance between operational practices and use of technology could potentially result in information vulnerabilities.

Table 1 summarizes the issues identified in this effort. "Operations and Technology" issues describe ways that the actions of individuals or the use of technology in telemedicine or telehealth encounters (and when telehealth technologies are used in traditional in-person care) could increase the vulnerability of PHI. "Public Policy" issues describe ways that federal or state regulation, or external certification or accreditation activities, might affect telemedicine or telehealth more directly than traditional in-person care. Note that a discussion of the Operational and Technical Issues is provided in Section II and a discussion of Public Policy Issues is provided in Section III.

Table 1 – Potential Privacy Issues in Telemedicine/Telehealth

Operations and Technology Issues (OT)
OT-1—Differences in cooperating locations' operational procedures and technology implementations could cause PHI exposure
OT-2—Some web sites may not adequately protect the PHI they collect
OT-3—Care delivery could be observed by unauthorized individuals without patient knowledge or permission
OT-4—Use of electronic messaging (e.g., e-mail) could expose PHI
OT-5—Electronic communications could be intercepted by people outside the care delivery domain
OT-6—Locally stored PHI could be accessed or altered by people with "system-level privileges"
Public Policy Issues (PP)
PP-1—Telemedicine/telehealth dependence on electronic media means that extensive preparation will be required to comply with the proposed Security Standards
PP-2—Since any more stringent state law would preempt HIPAA's final Privacy Standards, providers that use telehealth technology could be subjected to inconsistent requirements across their practice areas
PP-3—Practices of many health-related web sites are not subject to PHI privacy requirements
PP-4—Use of overly specific regulatory language about technical methods for protecting PHI could limit potential for using innovative solutions

Recommendations

Through interviews with representatives of leading organizations that deliver care using telemedicine and telehealth technologies,[9] we learned of excellent approaches for addressing the potential vulnerabilities identified in this report.

[8] "Covered entities" are health plans, healthcare clearinghouses, and healthcare providers who transmit any health information in electronic form in connection with certain transactions to carry out financial and administrative activities related to healthcare. Ibid. 45 CFR § 160.103 Definitions (see "covered entity" and "transaction").

[9] University of Tennessee Telemedicine Network, Marshfield Clinic TeleHealth Network, University of Virginia Commonwealth University School of Medicine, Missouri Telehealth Network, Alaska Federal Health Care Access Network, Rural Eastern Carolina Health Network, etc.

In many cases, the methods validated at those sites formed the basis of our recommendations. It is reasonable to expect that many recommendations documented here are currently being addressed in healthcare organizations' operating policies and procedures—or soon will be as the result of site efforts to ensure compliance with the latest regulatory requirements for protecting privacy of patient health information.[10]

The following recommendations describe actions that will aid in ensuring privacy of patient information during telemedicine/telehealth practice (and where comparable circumstances exist in traditional in-person care). Because some issues identified in this research are complex, their mitigation might require that a number of related actions be taken to address them; for this reason, note that the explanation of each recommendation begins with an indication of the telemedicine/telehealth issue(s) that incorporate the recommendation as a component of their resolution approach.

Operations and Technology

Recommendation 1: Ensure procedures implemented to protect PHI are compatible across sites

(Relates to Operational/Technical Issue 1)

Organizations working together to conduct telemedicine/telehealth should follow operational procedures that are tailored to the characteristics of their cooperative environment. The shared procedure implemented should ensure PHI privacy at each of the locations and in the communications environment that connects them. The approved procedures should govern both the circumstances where organizations cooperate in established formal relationships and where the organizations or their individual staff members cooperate in less formal (or even one-time) relationships. Each organization should ensure that the approved procedures are followed by its staff and update the procedures when operational or technical change is implemented at either location.

Recommendation 2 Implement a strong information privacy culture among the locations that share PHI

(Relates to Operational/Technical Issues 1 and 6)

Organizations should establish a foundation of strong privacy values throughout their shared telemedicine/telehealth environment using techniques such as: including PHI protection requirements in procedure documentation and job descriptions, reminding staff of their PHI protection responsibilities through training/retraining, requiring that staff sign PHI confidentiality agreements with the organization, and requiring PHI protection as part of Business Associate Agreements with the outside organizations that provide services to the telemedicine/telehealth environment. Taking actions such as these will orient non-clinical staff members to the privacy culture while also serving as a useful reminder to the clinical staff.

Recommendation 3 Ensure only authorized individuals can access telemedicine interactions/information

(Relates to Operational/Technical Issues 2, 3, and 6)

Organizations should utilize both procedure and technology to limit access to patient information. Clearly stated operational procedures will ensure that the staff associated with telemedicine/telehealth interactions comply with privacy requirements when executing their responsibilities. Physical security measures will protect the technologies used in delivering care and sharing information from harm and misuse. Implementation of technology to limit system access will provide services such as authenticating users, ensuring that users can

[10] For example, many healthcare organizations are conducting risk assessments of their operational environments using approaches that range from customized consultant-led investigations to internally managed studies.

access only information that is needed to perform assigned responsibilities, and logging users off the systems after a predefined period of inactivity. Periodic Risk Assessment evaluation of the operational environment will identify procedure- and technology-based weaknesses, and regular Vulnerability Assessments will identify potential weaknesses in the technical infrastructure. Intrusion detection systems will identify inappropriate system access and alert site authorities to potential security problems.

Recommendation 4
Protect privacy of patient information that is collected via web site interaction

(Relates to Operational/Technical Issue 2)

Organizations that use web sites to gather and maintain PHI should ensure protection of patient privacy by having strong controls over how communications are conducted and how collected PHI is handled. PHI-related web sites should meet the information protection requirements of the HIPAA Privacy Standards and proposed Security Standards regardless of whether the sponsoring organizations are HIPAA "covered entities."[11] In addition, the organizations should conform to guidelines for web site development/support and quality standards that are evolving within the healthcare industry through the work of various professional associations and commercial entities.

Recommendation 5
Select technology based on its ability to protect PHI

(Relates to Operational/Technical Issues 3 and 4)

Organizations should ensure the technologies they employ for processing PHI can be configured to provide the level of protection required for a telemedicine/telehealth environment. Where technological solutions are not available, are not cost-efficient, or would interfere with the quality of data storage or communications, healthcare organizations should implement highly specific operational procedures that will ensure adequate protection of PHI.

Recommendation 6
Implement procedure to control individual users' handling of PHI

(Relates to Operational/Technical Issues 3, 4, 5, and 6)

Organizations should establish procedures for their system users to follow when processing PHI outside the boundaries of the "controlled" healthcare application systems (e.g., their access-controlled clinical information systems). Procedure should outline requirements for handling electronic messages and attached files and, if the organization has extended its voice mail and facsimile technologies to interoperate with their e-mail systems, also address managing their e-mail-like voice and facsimile messages. To prevent equipment-based sources of exposure, organizations should consider denying PHI access by systems outside their direct control (e.g., by portable computers and personal digital assistants that "travel" with their users and by home and practice office computers that might be shared with individuals not authorized to access the organization's data).

Recommendation 7
Ensure communications approaches provide appropriate security for sharing PHI

(Relates to Operational/Technical Issues 2, 3, 4, and 5)

Organizations should protect their cross-site transfer of health information using mechanisms that offer a level of protection appropriate to (1) the clinical content of the interaction and (2) the communication method selected to carry out the exchange. For example, based on the perceived sensitivity of the information, an organization using or sending data over public systems or networks might consider using either encryption, application systems that have been designed to protect processed information, or Virtual Private Networks. When exchanging sensitive data with

[11] See footnote 8 for a definition of "covered entities."

web sites, an organization or individual might elect to use the Secure Socket Layer protocol.

Recommendation 8
Ensure compatibility of technical measures that sites implement to protect PHI

(Relates to Operational/Technical Issues 1 and 5)

Organizations should monitor effectiveness of the technical measures in use to protect information at each site and in the communications environment connecting them by regularly conducting vulnerability analyses to ensure their methods are not outdated.

Public Policy

Recommendation 9
Release latest plans for HIPAA Security Standards requirements

(Relates to Public Policy Issue 1)

Because extensive preparation might be required for organizations to achieve compliance with the detailed requirements of the Security Standards, HHS should promptly release information on plans for material changes to the regulation's current "proposed" language.

Recommendation 10
Encourage harmonization of state-federal law protecting privacy of patient information

(Relates to Public Policy Issue 2)

To relieve healthcare providers and organizations that deliver care across legal jurisdictions from having to identify and comply with state privacy laws and regulations that are contrary to and more stringent than HIPAA, HHS should encourage and sponsor a task force to promote harmonization of state and federal laws that deal with privacy of patient information.

Recommendation 11
Extend policy to protect PHI wherever it is collected, including web-based interactions

(Relates to Public Policy Issue 3; also see Operational/Technical Issue 2)

Healthcare and related industries should ensure through self-regulation that data defined by HIPAA to be "PHI" is appropriately protected by any organizations that collect it, even if the organizations are not subject to HIPAA. If this goal cannot be achieved through voluntary action, the government should issue policy that requires any organization that deals with the types of information that HIPAA classifies as "PHI" to protect it in ways that conform to the requirements placed on healthcare organizations by HIPAA and other privacy regulations.

Recommendation 12
Ensure policy statements define goals, permitting affected entities to select techniques

(Relates to Public Policy Issue 4)

Authors of policy should ensure that regulatory language clearly states the goal or requirement of the regulation and perhaps outlines mechanisms for detecting failure to meet that objective. Policy should refrain from specifying technique(s) to be used to satisfy the objective, leaving evaluation and selection of alternative approaches for achieving compliance to the affected entities.

Concluding Remarks

Our review of the processes, technologies, and communications employed in telemedicine interactions indicated, perhaps not surprisingly, that care delivered in traditional in-person settings is increasingly utilizing the same information technologies, communications tools, and support mechanisms that are employed to deliver care across a distance. Therefore, many potential vulnerabilities and recommendations described in this report are as relevant to traditional in-person care as to telemedicine and telehealth interactions.

Although extensive use of technology might establish the basis for many privacy issues, technology also provides many of the tools needed to address the issues. Most information privacy issues that might arise from using telehealth technologies in care delivery (whether

in telemedicine/telehealth interactions or traditional in-person care) can be addressed by defining and enforcing effective operational procedure, making effective use of technology, and promoting a culture of support for information privacy throughout the organization. Once initial compliance with privacy regulations has been established, maintaining compliance will require conducting periodic assessments of the effectiveness of procedures and technology use, performing case-by-case assessments of changes planned for the operational and technical environments, and continually adapting operational practices and technology implementations to maintain the balance between technology infrastructure and procedures established to guide staff members' work.

I. Introduction

This study addresses the portion of telehealth that relates closely to telemedicine, focusing on "the use of modern information and telecommunication technologies to provide health care services and access to health information…across a distance."[12] It evaluates information privacy issues associated with two aspects of telehealth: its care delivery component, also known as "telemedicine,[13 and 14] and its use of the Internet for care delivery and patient/consumer education. The evaluation does not address privacy issues shared with the broader environment of traditional in-person care, and it sets aside for separate study the components of telehealth that address research, education and training, and, to some degree, public awareness of health-related issues.

It is important to realize that electronic tools are becoming more generally available on clinicians' desktops, and use of these tools in traditional in-person care is growing to the point where it is often difficult to distinguish between telemedicine/telehealth and traditional in-person care delivery interactions. For example, two healthcare providers conducting a traditional in-person care consultation might employ e-mail for communication, or an in-person clinic visit might incorporate services of an off-site specialist to provide real-time interpretation and reporting of radiology exams. In both cases, the activity performed during delivery traditional in-person care is almost indistinguishable from telemedicine/telehealth activities.

This report outlines the information privacy, confidentiality, and security issues that are present when care is delivered across a distance and provides recommendations for improving the degree of protection afforded to patient information during this type of care delivery.

Information Privacy Regulatory Environment

As is true for traditional in-person care delivery, participants in telemedicine/telehealth interactions have a legal and ethical obligation to protect patient *privacy* by applying appropriate *security* safeguards to maintain *confidentiality* of information about the patient (Figure 1 provides "working definitions" of these terms[15]).

Privacy is an individual's claim to control the use and disclosure of personal information. This claim is backed by the societal value representing that claim.

Confidentiality is a status accorded to information that indicates it is sensitive for stated reasons and therefore must be protected and access to it controlled.

Security is the safeguards (administrative, technical, or physical) in an information system that protect it and its information against unauthorized disclosure (also protecting its integrity and availability), and limit access to authorized users in accordance with an established policy.

Figure 1 - Working Definitions: Privacy, Confidentiality, Security

"Many legal issues raised by telemedicine are not really new, but require the law to be applied in a new area. Now, in addition to the government, managed care companies, providers, and the public, many Internet companies are also accumulating health information about

[12] Excerpt from Puskin, Mintzer, & Wasem (1997, p. 276). See full definition of "telehealth" in footnote 1.

[13] One definition, and there are many, of "telemedicine" is "a subset of telehealth, allowing a clinician to provide care via telecommunications." Chaffee (1999).

[14] A brief overview of the practice techniques used in telemedicine/telehealth and a description of how these interactions differ from traditional "in-person" care delivery is provided in Appendix B.

[15] Provided by John Fanning, Privacy Advocate for DHHS, at the January 2001 "Privacy, Security, and Confidentiality of Medical Records" seminar for OAT grantees. Kumekawa (Feb. 18, 2000).

individuals, and much of it most people would consider private."[16] The 2001 Telemedicine Report to Congress notes, "The Internet will most likely play a key role in expanding the reach of telehealth and telemedicine to the average consumer," and it identifies "privacy, security, and confidentiality" as a key issue affecting the industry.[17]

An important component of the telemedicine/telehealth policy environment is the guidance for protecting the privacy and security of healthcare information that was issued by the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). (See Appendix A for an overview of subjects addressed by HIPAA.) Provisions of the HIPAA Privacy Standards[18] require protection of health information that is created or maintained by "covered entities," (i.e., healthcare providers who engage in certain electronic transactions, health plans, and healthcare clearinghouses), regardless of the form in which the information is used—on paper, electronically, and verbally. Administrative Requirements of the Privacy Standards require that "A covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information."[19] Most organizations covered by the Privacy Standards must comply by April 14, 2003.

Provisions of the proposed HIPAA Security Standards,[20] in Notice of Proposed Rule Making (NPRM) status as of this writing, will apply to the same organizations as the Privacy Standards, setting guidelines for these organizations to develop and maintain the security of their electronic individual health information. The proposed Security Standards outline specific requirements and suggest alternative techniques for implementing the Privacy Standards' directive. The components of the proposed Security Standards actually reflect standards and procedures that are generally accepted as "best practices" for providing a secure information processing environment,[21] making its direction useful as a guideline for proper internal procedure despite the NPRM status.

Overview of Telemedicine/Telehealth Care Delivery Interaction

Study of protocols for delivery of care across a distance in Radiology, Mental Health, Dermatology, Home Health, and other clinical specialties indicated that practitioners of these diverse clinical specialties perform telemedicine interactions in similar ways. Differences in styles of telemedicine interaction related to the subjects discussed and the types of medical peripherals employed for examining the patient—not to the specialties, the telemedicine technologies selected for the interaction, or the sequence of activities followed to deliver care. This report's security, privacy, and confidentiality issues and recommendations are applicable across the clinical specialties and do not focus on one specialty more than another.

As illustrated in Figure 2 and described below, the study noted that three styles of electronic information exchange are commonly employed for telemedicine and telehealth interactions:

- **Interactive videoconferencing** uses real-time transmission of sound and video images

[16] Ibid.

[17] Puskin & Kumekawa (2001, p.1).

[18] Standards for Privacy of Individually Identifiable Health Information (2000).

[19] Ibid. 45 CFR § 164.530(c)(1).

[20] Security and Electronic Signature Standards (Proposed Rule) (1998).

[21] The proposed HIPAA Security Standards align closely with guidelines for security practice recommended by authoritative sources such as the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. See Swanson (1996) and An Introduction.

between sites to support patient-provider or provider-provider interaction that is similar to visits conducted in healthcare providers' offices. The interaction might also include use of medical peripherals—such as an electronic stethoscope—to transmit certain types of patient vital signs.

- **Store & forward messaging** is an electronic correspondence, often with clinical documents and images attached to the messages, that is conducted between two providers or a provider and patient.
- **Web site interaction** is a correspondence in which one of the participants is a public or private web site.[22] When conducted as a telehealth interaction, the exchange typically involves a patient or consumer accessing a health-related web site via the Internet and providing certain health-related information; the web site, using software-only or an interface that includes human response, responds with health- or care-related information.

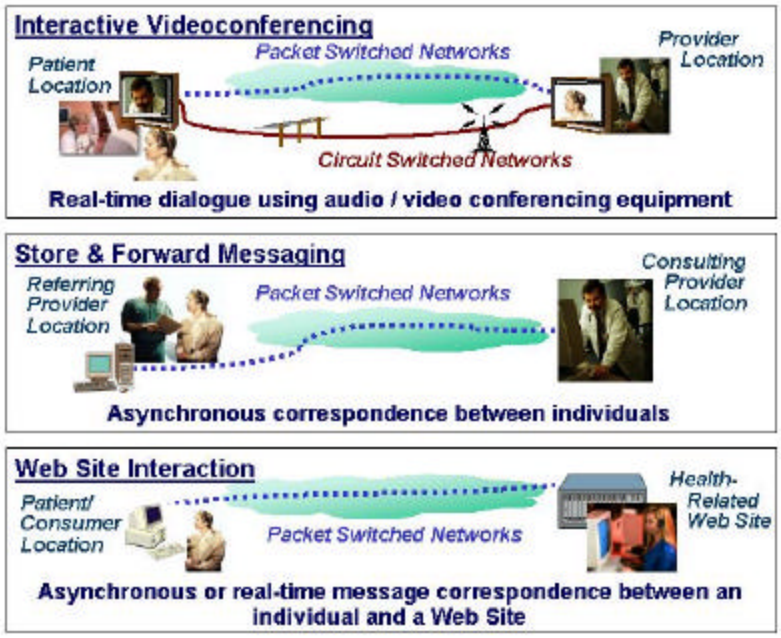

Figure 2 - Common Styles of Telemedicine/Telehealth Interaction

While each style of interaction is used extensively, the selection of one or another for a particular exchange is dependent on considerations such as the clinical characteristics of the interaction, availability of the requisite supporting technologies, and personal preference of the individuals involved.[23] As true for clinical specialties, the security, privacy, and confidentiality issues and recommendations provided in this report are not more applicable to one of the interaction approaches than the others.

Activities of a Telemedicine Interaction

The authors developed scenarios for five types of telemedicine and telehealth interaction based on information gathered from interviewing individuals who provide care via telemedicine interaction. Most scenarios had three phases—*arranging* for the interaction, *conducting* it (which might be carried out as a series of

[22] Literature reviews revealed the rapid growth of this style of telemedicine interaction as an emerging, widely used mechanism for care delivery and access to health information.

[23] For example, a healthcare provider might prefer to use interactive videoconferencing for a patient encounter because it is important to observe the patient's behavior and movement during the verbal interchange. Alternatively, the provider might prefer to use store & forward when the work involves activities such as examining an image or document and responding with an opinion. A patient or consumer might prefer web site interaction as a way to obtain useful health-related information quickly and/or anonymously.

interactions), and *documenting* the result of the interaction (or the series).

Activities of an encounter are illustrated in Figure 3, which summarizes the phases and activities of a typical encounter between provider and patient that is conducted using interactive videoconferencing technology. (It also indicates, with shaded boxes that have darker borders, the subset of activities that would occur in a provider-provider consultation.) Activities depicted in the figure are summarized below:[24]

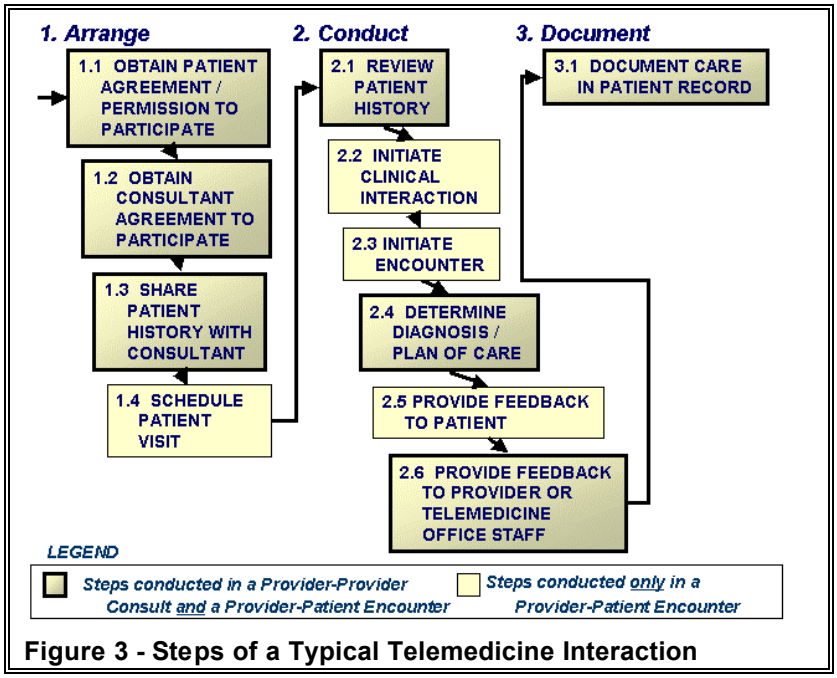

Figure 3 - Steps of a Typical Telemedicine Interaction

- **Arrange:** Activities to *Arrange* for a telemedicine interaction begin when a referring provider and the patient discuss the need to consult another provider for medical advice or opinions. The referring provider explains to the patient that the encounter will be conducted from a telemedicine-equipped site in the local area, identifies who will serve as the consulting provider, discusses the organization's Notice of Privacy Practices (NPP) with the patient, and obtains the patient's signed acknowledgement indicating understanding of the NPP. The referring provider discusses the case with the consultant (and might use store & forward techniques to send relevant patient medical data to the consultant) and takes appropriate steps to schedule the interaction to occur at a telemedicine provider site in the community. ("Scheduling" involves setting a time when the necessary elements of the interaction—patient, consultant, and essential resources such as staff, video-equipped rooms, and appropriate medical equipment—are all available.)

- **Conduct:** Activities to *Conduct* the interaction might occur only once, or might (if authorized by the referring provider) be repeated for a series of visits. The interaction begins with the consultant reviewing the patient's clinical history and, if necessary, requesting additional information from the referring provider. Upon arriving at the local telemedicine site, the patient signs forms as appropriate (e.g., the site's NPP, registration forms, and/or consents) and receives some orientation to the consult room and the telehealth technologies. Next, telehealth technologies are utilized to establish an interactive videoconferencing connection between the consulting and patient sites. The patient and consulting provider introduce themselves and any other individuals who are in the consult rooms, and the patient indicates who may be present during the encounter. If appropriate, the staff arranges for the patient to sign an Informed Consent for the procedure. Consultant and patient then discuss the patient's clinical problems, medical history, etc., and the consultant determines the diagnosis and plan of care. The consultant develops recommendations (e.g., diagnosis, treatment plan, prescriptions, and a decision about

[24] For a more detailed description of these steps, see Section III-Generalized Telemedicine Interaction Scenario in Volume 2 of this report.

whether a follow-up visit should be scheduled), discusses the recommendations with the patient, communicates orders for new or changed plan of care to the patient and telemedicine site staff, and terminates the session. To conclude the visit, staff of the local telemedicine site order/fill prescriptions and schedule a follow-up appointment if appropriate, and the patient leaves the site.

- **Document:** Activities to conclude, or *Document*, the interaction begin upon completion of the encounter (or authorized series of encounters). The consultant prepares the Consult Report summarizing the case, has it transcribed, and forwards it to the referring provider. The encounter is formally concluded when both providers have appropriately filed or disposed of documentation related to the case.

Report Organization

This report is published as two volumes:

- **Volume 1 – Issues and Recommendations** provides the observations and conclusions of this study. Section I provides context for conducting the study, Section II describes information privacy issues for operational practice and technology used in telemedicine/telehealth care delivery, Section III summarizes circumstances where public policy might be altered or enhanced relative to telemedicine/telehealth, and Section IV provides the conclusions of the study and a summary of the recommendations for reducing vulnerability of health information when delivering care using telehealth technologies. At the end of the volume, References/Bibliography provides a comprehensive list of the references and communications used during the study, and the Appendix provides a summary of the HIPAA regulation and a list of the abbreviations and acronyms used in the report.
- **Volume 2–Telemedicine/Telehealth Interaction Scenarios** provides research materials developed during the study.

Following the Introduction, it provides an overview of how care is delivered using telemedicine and telehealth technologies. Next, it provides overviews of how telemedicine interactions are conducted:

- The Generalized Telemedicine Interaction Scenario section provides a typical *generalized* telemedicine scenario, indicating information vulnerabilities that could potentially be associated with each activity and summarizing current and proposed policy that applies to the activity;
- The Telemedicine/Telehealth Scenarios section provides a synopsis of how five types of telemedicine and telehealth interactions are conducted:
  - Interactive Provider-Patient Encounter,
  - Non-interactive Provider-Provider Consult,
  - Interactive Provider-Patient Home Health Encounter,
  - Non-interactive Computer-Computer Home Health Data Upload, and
  - Non-interactive Patient-Web Provider Encounter.
  - Each scenario lists the major activities, information vulnerabilities that might be associated with the activities, and recommendations for protecting privacy of patient information during the interaction.

II. Operations and Technology Issues and Recommendations

Introduction

The telehealth-unique information privacy issues identified in this study relate directly to "the use of modern information and telecommunications technologies to provide healthcare services…across a distance."[25] Healthcare is rapidly adopting new electronic information technology capabilities to provide improvements in operational efficiency and quality of work. As is true in almost every other industry, the implementation of new technology often occurs more rapidly than implementation of the security measures and procedures necessary for appropriately controlling its use. The core observation of this study is that a healthcare organization's information privacy culture and information protection capabilities are highly dependent on its operational practices, leading to the broad recommendation that an organization must continually adapt operational practices to maintain a balance between its frequently changing technology infrastructure and the procedures implemented to guide staff activity.

The HIPAA Privacy Standards and proposed Security Standards establish highly specific guidelines for information protection and describe specific penalties for information exposure. Two elements of the HIPAA legislation form the basis of most issues identified in this section: the Privacy Standards state that appropriate administrative, technical, and physical safeguards must protect the privacy of PHI,[26] and the proposed Security Standards support the Privacy Standards requirement by outlining the types of procedures and processes that should be implemented to protect the integrity, confidentiality, and availability of electronic information.[27]

Providers conducting either telemedicine or traditional in-person care interactions utilize their organizations' "controlled" clinical application systems where possible.[28] However, whether by choice or necessity, the providers might also share patient information with each other outside the boundaries of the controlled systems. Providers are gradually migrating from use of communications practices that have long been considered "safe" by the industry and regulators (e.g., facsimile, telephone, and the mail) to tools such as e-mail that are readily accessible on their electronic desktops. The non-clinical desktop tools do not provide the type of PHI-related protections that are designed into the controlled clinical application systems. In addition, their use places a significant amount of PHI into their organizations' non-controlled technical infrastructures (e.g., the file servers, e-mail systems, the communications infrastructure, etc.) where it might be readily accessible to entities outside the clinical environment.[29]

---

[25] Excerpt from the definition of "Telehealth" from Puskin, Mintzer, & Wasem (1997, p. 276).

[26] Standards for Privacy of Individually Identifiable Health Information (2000), 45 CFR § 164.530(c)(1).

[27] Security and Electronic Signature Standards (Proposed Rule) (1998), 45 CFR § 142.308(d), Technical Security Mechanisms.

[28] Many healthcare organizations implement "controlled" clinical applications that have built-in information protection capabilities including user authorization (e.g., user ID/password to sign on) and access control (e.g., role-based access limiting a user's view of patient information to data that is essential to performance of his or her job duties). Also, they usually manage the technical support of these controlled clinical systems differently from support of non-clinical applications, assigning the responsibility to staff members who are specially trained in patient privacy requirements and ways to ensure data in the system is properly protected.

[29] A number of these issues and options for addressing them are discussed in Tabar (2002).

Issues and Recommendations

1 - Differences in cooperating locations' operational procedures and technology implementations could cause PHI exposure

Issue: Even when work processes in a healthcare organization are performed according to procedures that ensure privacy of PHI,[30] patient information could be exposed when organizations or individual providers cooperate to deliver care across a distance in a telemedicine/telehealth interaction. The information exposure could be caused by differences in operational or technical procedures at the locations, or it could result from interaction of the hardware and software products employed in the locations' communications and technical infrastructures.

Recommendation: Organizations and individuals must be diligent in ensuring that their combined resources are applied appropriately for protecting information in their shared telemedicine/telehealth infrastructure—at each location and in the communications environment that connects them. The organizations should take the following steps to protect PHI during their telehealth interaction:

- Develop and agree on a shared operational procedure for conducting secure care delivery interactions, and even identify the need for special physical security measures at the locations involved in the telemedicine/telehealth interactions;
- Ensure that the technical components of the shared environment, including the communications technology, computer hardware and software, and often even the parameter settings of these components, are implemented so that the devices interoperate effectively and provide appropriate levels of security;
- Maintain an ongoing collaboration to evaluate whether planned changes will affect security of the shared technical environment, and take appropriate action to eliminate, reduce, or manage new vulnerabilities that are identified; and
- Ensure the procedures developed to protect information in the shared telemedicine/telehealth environment are followed.

As a foundation for the shared procedure, the organizations should ensure that they maintain a culture of confidentiality throughout their operation. Many effective techniques exist for promoting privacy values, particularly the following:

- Clearly state requirements for protecting PHI in the context of procedure documentation and staff members' job descriptions;
- Remind staff members of PHI protection responsibilities through training[31] and periodic retraining; and
- Require staff members to sign, and periodically re-sign, agreements in which they commit to protecting the privacy of the organization's PHI.

[30] A healthcare organization delivering care by traditional means expends significant effort to establish operating policies and procedures for protecting privacy of patient information, considering operational procedures, technologies employed, facility planning, and even paper forms that are used. In addition, they monitor staff execution of responsibilities to determine whether procedures are followed and identify areas where improvement is needed.

[31] "In determining what training should be provided…remember that the message will be different for different users…management needs to understand HIPAA from a strategic, budgetary and liability perspective; the needs of a hospital volunteer would be much simpler." Gue (2002).

When external resources are utilized as an extension of the workforce (e.g., to provide services such as computer support or patient care), requirements for PHI protection should be stressed in their Business Associate Agreements, specific procedures and penalties should be outlined, and staff of these organizations should be made subject to the same procedure, job description, training, and privacy commitment procedures as the organization's own staff members. Organization-wide promotion of an ethic that requires PHI protection regardless of where information resides will orient the non-clinical staff members to this requirement while also serving as a useful reminder to clinical staff and will provide a sound basis for individual decision-making as staff members face new situations and challenges.

2 - Some web sites may not adequately protect the PHI they collect

Issue: Some web sites that gather and maintain an individual's health information do not ensure that the privacy of that information is protected. Sometimes this is due to improper or careless use of the new, frequently changing web-based technologies.[32] Often, however, it is because many organizations that collect information are not subject to HIPAA.[33] Although standards for the development and ongoing support of web sites that collect PHI are evolving through the work of various organizations, compliance is voluntary and enforcement receives only limited attention. Regulatory authorities have neither mandated standards and procedures for ensuring protection of web site data nor identified methods for assuring compliance. (Note that this report does not address the potential use or misuse of the Internet for unethical collection of PHI or any other unethical health-related purposes.)

Recommendation: Regardless of whether the sponsoring organizations are covered entities subject to HIPAA, the organizations that sponsor collecting health information from individuals via the web should ensure they are providing appropriate levels of protection for the PHI they acquire. These organizations should implement operational and technical procedures that conform to information protection guidelines set for healthcare organizations by the HIPAA Privacy Standards and the proposed Security Standards; further, they should implement procedures for to website development and support that are based on measures recommended in guidelines currently under development by numerous healthcare industry professional associations and commercial entities.[34]

---

[32] See O'Harrow (2001) for a report of Eli Lilly and Co. inadvertently releasing e-mail addresses of over 600 people who had subscribed to a Prozac-related e-mail service. Also see Piller (2001) for a report of an accidental web posting of detailed psychological files of 62 children and teenagers.

[33] "…the same activities conducted at different Web sites will be subject to different legal treatment. Specific activities—ordering a prescription, getting a second opinion, consulting with a doctor, or even maintaining a medical record—may be covered by the new regulation at one Web site and unregulated at another." Choy, Hudson, Pritts, & Goldman (2001, pp. 7-8). Also, see footnote 8 for a definition of HIPAA "covered entity."

[34] Useful guidelines for development and use of PHI-related web sites are provided by some healthcare organizations, for example, URAC (the American Accreditation HealthCare Commission) and the eRisk in Healthcare Project (of the eRisk Working Group for Healthcare sponsored by Medem, Inc. on behalf of a large number of medical societies). Choy, Hudson, Pritts & Goldman (2001, p. 24) provide pointers to the following "standards and seal programs to address privacy, security and quality on the Internet: Standards and seal programs that are in development or have been developed include: Association of American Health Plans, *AAHP Principles for Consumer Information In an E-Health Environment*, http://www.aahp.org; American Health Information Management Association, *Recommendations to Ensure Privacy and Quality of Personal Health Information on the Internet*, http://www.ahima.org/infocenter/guidelines/tenets.html; Health On the Net Foundation, *HON Code of Conduct*,

(Footnote continues on next page.)

3 - Care delivery could be observed by unauthorized individuals without patient knowledge or permission

Issue: In traditional in-person care delivery, a patient is generally able to identify when persons other than the provider are present in the treatment room and then decide whether to permit their presence during care delivery. Care delivery using electronic information and communications technologies does not intrinsically offer the same level of privacy, as described below:

- The patient in an interactive video encounter must depend on introductions and/or viewing the distant location through the camera lens to detect presence of uninvolved personnel such as medical students, assistants, or other types of observers. Also, the patient typically has no mechanism for detecting presence of individuals who provide technical support for conducting the interaction.
- Depending on the telemedicine organization's procedures, activities associated with scheduling the people, equipment, and rooms in multiple facilities for a telemedicine appointment might cause some exposure of PHI to unauthorized individuals. While this is also a concern for traditional in-person care, there could be additional potential for exposure if the telemedicine scheduling conversations must be conducted with multiple sites.[35]
- When store & forward messaging techniques are used for a telemedicine interaction, it is possible for communications to be observed by individuals who are not care delivery participants—for example, communications service providers, site staff members, and even unauthorized individuals who have inappropriately gained access to the systems or communications environments of the sites. Additional types of exposure could occur if one or both parties participate from a home or personal office instead of from a location that is under the direct control of a healthcare organization.

Lawyers specializing in the study of HIPAA implications[36] have interpreted the HIPAA Privacy Standards' requirement that covered entities obtain written or verbal permission to use or disclose protected health information to mean that third parties who are not present to assist in the care of the patient may not participate without patient authorization. Therefore, if individuals present at the distant location are not introduced, or if unauthorized individuals intercept or monitor health-related communications, the patient is not afforded the legal right to permit or

http://www.hon.ch/HONcode/Conduct.html; Hi-Ethics, *Ethical Principles For Offering Internet Health Services to Consumers*, http://www.hiethics.org; International Society for Mental Health Online, *Suggested Principles for the Online Provision of Mental Health Services*, http://www.ismho.org/suggestions.html; Internet Healthcare Coalition, eHealth Ethics Initiative, *eHealth Code of Ethics*, http://www.ihealthcoalition.org/ethics/ethics.html; National Association of Boards of Pharmacy, Verified Internet Pharmacy Practice Sites program, http://www.nabp.net; National Board for Certified Counselors, *Standards for the Ethical Practice of Internet Counseling*, http://www.nbcc.org/ethics/webethics.htm; TRUSTe and Hi-Ethics, E-Health Seal Program, http://www.truste.org/programs/pub_ehealth.html; URAC and Hi-Ethics, Health Web Site Accreditation, http://www.urac.org/programs/technologyhws.htm; and M.A. Winker et al., *Guidelines for Medical and Health Information Sites on the Internet,* American Medical Association, 283 JAMA 1600 (2000), http://www.ama-assn.org/ama/pub/category/1905.html."

[35] To preclude this type of exposure, some organizations ensure that they schedule telemedicine visits using the same procedures and resources that arrange for traditional care referrals. For example, the Missouri Telehealth Network website's "How to Schedule a Patient" instructions note that "there is no difference in the manner in which an in-person Dermatology appointment or a telehealth Dermatology appointment is scheduled." See "How to Schedule."

[36] Waters & Spencer (2001). See Volume 2, Generalized Telemedicine Interaction Scenario, Step 2.2.e.

deny their presence and the patient's PHI would be inappropriately exposed to these individuals.

As is true for providers who practice traditional in-person care and are subject to the same sanctions under law, "telemedicine/telehealth providers who expose health information to unauthorized individuals, intentionally or negligently, could be subject to a variety of liability laws and privacy laws other than HIPAA." It is also possible that liability and privacy regulations that are not healthcare-specific might be applied, such as state consumer protection laws, claims for negligence or other tort claims under state law, violation of the Medicare and Medicaid program Conditions of Participation that include privacy protections, and contractual violations caused by contract provisions that include obligations to provide privacy protections.[37] Still other privacy-oriented regulations might be applied to care interactions, as described below:

> "Another area of potential liability is enforcement action by the Federal Trade Commission. Although the FTC lacks any statutory mandate to address healthcare privacy issues, the FTC has indicated that representations regarding privacy that are published in the Internet (such as a notice of privacy practices under HIPAA) could, if violated, give rise to enforcement actions by the FTC against the alleged violators, in the nature of unfair and deceptive trade practices.
>
> "It should also be borne in mind that the state Boards of Registration that license healthcare professionals, and other state authorities that license non-healthcare professionals who interact with healthcare professionals, could look to HIPAA for guidance and as a foundation for determining whether allegations of privacy violations are worthy of investigating. Thus an alleged violation of a HIPAA rule provision, looked to by analogy by a state Board of Registration in Medicine or a Board of Bar Overseers, could result in loss of licensure for a physician or loss of bar admission for a lawyer."[38]

Recommendation: Organizations that deliver care using electronic information and communications technologies should implement operational procedure to ensure that privacy of patient information is maintained. For example:

- Implement physical security measures to protect resources used in delivering telemedicine care (e.g., locking rooms used for telemedicine interaction when not in use, preventing unauthorized access to workstations used to deliver care via store & forward or web site interaction, etc.);
- Employ operational procedure that ensures staff comply with privacy requirements when performing their work responsibilities (e.g., introduce all individuals present at locations participating in a telemedicine exchange and comply with the patient's direction about observers and non-essential personnel who may remain or must leave; also, conduct interactive videoconferencing, appointment scheduling, and other care-related conversations in locations that offer reasonable privacy safeguards); and
- Use a shared secure computer system for scheduling appointments to reduce the need for conversation and limit access to the information.

As is true for traditional in-person care, the organizations should also implement technical measures to secure their operational environments

[37] Goldberg (May 17, 2002).

[38] Ibid.

against unauthorized individuals accessing patient information, including:

- Prevent unauthorized, unauditable access to care providers' workstations through controls such as strong user authentication techniques (smartcards or biometrics that verify the identity of the individual requesting access) and automatic system logoff (that prevents unidentified and unauthenticated individuals from using an active session by automatically ending it after a specified period of time or when the user is no longer in proximity to the workstation);
- Implement electronic signature for extremely sensitive or high-risk communications to verify the originator of a message and utilize encryption to preclude message receipt by someone other than the intended recipient; and
- Ensure that contracts and Business Associate Agreements with providers of technical services (e.g., videoconferencing bridge, technical support for computer/communications technologies, etc.) impose the same PHI protection responsibilities that are in place for site personnel.

Organizations should identify weaknesses in their operations on a regular basis by conducting information risk assessments, executing vulnerability assessments of their technical environments, and utilizing intrusion detection systems to identify inappropriate access to systems and alert authorities.

4 - Use of electronic messaging (e.g., e-mail) could expose PHI

Issue: Many telemedicine interactions occur as a store & forward exchange of electronic messages such as e-mails, often with documents and files attached to them. "E-mail is the single largest unprotected application that exists in the corporate world today… susceptible to four types of attacks: eavesdropping, forgery, denial of origination and reply."[39] The susceptibility of electronic messages to unintended exposure is highly dependent on how the correspondents manage them and how the site's technical support procedures and staff protect them. The high level of e-mail vulnerability has caused the American Medical Association to "…encourage physicians to select a secure messaging solution, rather than use un-secure e-mail, which is not encrypted and similar to sending a postcard."[40]

Unlike environments where the controlled clinical information systems provide intrinsic PHI protection capabilities, in electronic messaging it is the individual correspondents (e.g., the healthcare providers) who carry primary responsibility for managing both interim and final disposition of their e-mails and the documents attached to them. Unless these individuals handle messages very carefully, the PHI contained in the messages could be intentionally or unintentionally stored in a number of non-secure places in the computer environment of both sender and recipient. For example, the messages might be:

- Archived on the e-mail system server, network file servers, hard drives of individuals' workstations, and even on individuals' home computers;
- Retained (unnoticed by the correspondent) in certain "system" areas of the computers that processed them (e.g., in various "TMP" temporary storage locations, in the e-mail system's "Deleted," "Draft," and "Sent" folders, etc.); and
- Retained (in accordance with established technical support procedures at the participating

[39] Quote of Steve Gersten of Zixit Corporation in "E-mail Security," (2001, p. 25).

[40] Quote of Donald J. Palmisano, MD, AMA Trustee and member of the AMA Online Oversight Panel in "Avoid Standard Un-secure E-mail," (2001).

healthcare organizations) on system backup files for the email system server, the network file servers, and even the hard drives of the individuals' workstations.

PHI is accessible from each of these repositories by authorized and unauthorized individuals, for viewing or sending to others. Use of techniques such as password protection of saved files might limit access to some saved PHI, but would fail to protect any copies that were inadvertently left in other locations on the participants' computers or along the communications path. Typically, organizations do not know if they have a serious problem in this area because they rarely undertake the extremely labor-intensive task of determining how well individuals comply with proscribed local procedure (if it exists) for managing e-mails that contain PHI.

The e-mail/attachment vulnerability also occurs in relation to some other common forms of communication, specifically where organizations have taken advantage of the operational efficiencies realized from expanding their e-mail systems to support the electronic message implementation of voice mail and facsimile. Where this has occurred, these voice and paper messages that have generally been considered "safe" in transit and at their destinations are converted to electronic messages. Unknown to the sender, these messages assume processing characteristics similar to e-mails, meaning that the messages could be accessed from multiple locations and digitally stored, copied, and forwarded.

Recommendation: Organizations should establish certain technical and operational practices that will help to reduce inadvertent exposure of PHI during electronic messaging. For example:

- Clearly state in operational procedures whether it is permitted for e-mails and attached documentation to contain PHI. If the practice is permitted, specify how system users are to manage their e-mails and attached documentation,[41] and monitor user activities to ensure compliance. Also, consider the use of simple techniques such as assuring that clinical information is communicated separately from a patient's identity, each message including a unique identifier that is not traceable to the patient's identity for the recipient to use in re-associating the information.
- Require and, where possible, automatically ensure[42] that electronic materials containing PHI are protected (e.g., by encryption) prior to being sent offsite or saved on local e-mail and file servers. When deciding whether to employ encryption for internal and/or offsite e-mails and how to implement it, evaluate and address any technical issues that such a solution might create for other aspects of the systems support environment. (For example, it might not be possible for the organization's firewall/systems software to determine whether encrypted e-mails contain viruses.[43])
- Prevent computers that are not resident at the site and under the organization's direct control

[41] Useful sources of information for e-mail guidelines have been published by authoritative healthcare sources, including: American Medical Association in "Guidelines for Physician-Patient…," (n.d.), http://www.ama-assn.org/ama/pub/category/2386.html; Federation of State Medical Boards in "Model Guidelines" (2002), http://www.fsmb.org, follow link to Policy Documents; Massachusetts Health Data Consortium in Sands, (n.d.), , http://www.mahealthdata.org follow link to Patient-centered E-mail Guidelines; Journal of the American Medical Informatics Association in Kane & Sands (1998), http://www.amia.org/pubs/other/email_guidelines.html; and American Health Information Management Association in "Practice Brief" (2000), http://www.ahima.org/journal/pb/00.02.html.

[42] Several firms have developed technology that will either allow or force encryption of e-mail traffic. Examples of such technology reinforcement include: Zixit (see www.zixit.com) and Weblock (see www.securepath.com).

[43] Tabar (2002).

from accessing the organization's systems and files that contain patient information. That is, deny system access for devices such as laptop computers and Personal Digital Assistants that "travel" with users, home and practice office computers that the provider might share with other (unauthorized) individuals, etc.

Implementation of these types of controls will allow organizations to improve the level of protection afforded to the PHI that is processed outside the protection boundaries of their "controlled" clinical systems.

5 - Electronic communications could be intercepted by people outside the care delivery domain

Issue: Electronic communications are subject to interception—both internally at the locations participating in telemedicine/telehealth interactions and externally during transfer of information between locations. The interception might acquire a data or eavesdrop on audio transmission, or it could extend to viewing an entire audio/video care delivery process. In general, information placed into communications networks is vulnerable to interception by unauthorized individuals at the points where it enters or leaves a device on the communications path. For example:

- **On wire-based telephone circuits**, the threat of interception is generally considered to be minimal because access is regulated and tightly controlled by the common carriers. One point of potential vulnerability, however, is where a third party service known as a "communications bridge" is employed to link multiple participants into a single call; it is possible for a motivated individual at the bridge site to place eavesdropping equipment on the communication. Another potential vulnerability is at the healthcare sites, where a motivated individual could intercept communications using methods such as listening on an extension telephone line or placing eavesdropping equipment on a site communication device.
- **On networks with wireless components**, both the signals generated by individual transmitters (cellular telephones, wireless workstations, radio transmitters, microwave relays, etc.) and the signals passed along the wireless network (via relays, routers, hubs, cell sites, etc.) are generally susceptible to interception. Although the newer digital technology offers relief from analog technology's susceptibility to inadvertent disclosure, present standards for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants, and other wireless terminals (e.g., the standard known as Wireless Application Protocol) have proven subject to intentional interception.[44]
- **On wireless satellite or microwave radio links of long-haul communications systems**, it is possible, although difficult, for a motivated individual to monitor communications without detection. To intercept such a communication, the eavesdropper would have to overcome significant technical barriers (e.g., frequency division, time division, code division, composite video, and/or use of asynchronous transfer mode) that the various communication protocols incorporate into the wireless relays. Total reliance on these communication protocols for protecting sensitive traffic is "security by obscurity" and not a complete barrier against a determined eavesdropper.
- **On packet data networks**, transmitted information is briefly stored on every device along its communications path—at the sending sites, at nodes that comprise the communications path between the sites, and at the receiving site. Since information could be

[44] Salkever (2001); Verton & Brewin (2001); and Radcliff (2001).

intercepted as it passes into or out of any device along the path, exposure is very possible.

Network providers guarantee intrinsic security to protect the network's integrity, confidentiality, and availability. However, recognizing that some communications content might require higher assurance of protection, these providers also offer fee-based security services (e.g., copper/fiber wire-line link assurance and encrypted radio wave links) and features (e.g., encryption devices at video bridging facilities). Fee-based network security services (e.g., Virtual Private Networks) operate at sufficient speed to support most current broadband communication requirements. The alternative to total reliance on network security is user-provided, application-specific security (e.g., session encryption). Application security provides "end-to-end" security regardless of the presence or absence of network security, but it also carries an overhead cost that might affect quality of service.

Recommendation: To protect communications from interception, healthcare organizations must control and appropriately limit access to communications devices and pathways by their staff, by contracted service providers, and by strangers. Methods for doing this vary, based on the types of technologies employed and the communications carriers available in the affected geographic areas. For example:

- **User Practices:** In general, the individuals who use PHI during interactive videoconferencing, store & forward messaging, and/or web interaction should not have to become technically expert on how to protect it. Instead, healthcare organizations should provide their users with proven, "best practice" procedures to follow so the users exercise an established technical infrastructure and are automatically insulated from exposing information.
- **Infrastructure Support:** Organizations should protect electronic communications using methods that are appropriate to the sensitivity of the information being transmitted. As a general model for securing communications, sites should strive to achieve the "best practice" described in the proposed HIPAA Security Standards—that is, "protection of sensitive communications transmissions over open or private networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient."[45] For example:
  - For voice and video communications that utilize third party "bridge" services to connect the participating locations, including privacy requirements in Business Associate Agreements with the third parties will ensure that content of the communication is kept private.
  - For data communications over public networks such as the Internet (e.g., e-mails), use of encryption will protect against interception.
  - For point-to-point exchange of sensitive information over public networks, use of customized applications that provide protection during communications, or use of Virtual Private Network (VPN) communications services, will reduce the likelihood of exposure during verbal communications, data communications (e.g., store & forward messaging), and interactive videoconferencing.
  - For communicating with web sites, use of protection mechanisms such as the accepted security standard called "Secure Socket Layer" (SSL) will protect information from exposure enroute. (As of this writing, SSL is the minimal standard for all occasions where personal or personally identifiable information is exchanged over public networks; note that use of SSL does not provide any protection for data at the

[45] Security and Electronic Signature Standards (Proposed Rule) (1998), 45 CFR § 142.308(d), Technical Security Mechanisms.

sending or receiving sites—that protection must be provided through use of effective site practices and policies.)

6 - Locally stored PHI could be accessed or altered by people with "system-level privileges"

Issue: The systems support staff of a healthcare organization (i.e., the people who are responsible for assuring that site data and communications infrastructures operate properly and are protected) must know every element of how the infrastructure works and must have access to the infrastructure components and their contents to investigate and fix any problems that are reported. The broad information access rights (known as "system-level privileges") that are accorded to the systems support staff apply to the organization's communications and systems environments, to information stored on file and e-mail servers and their backup files, and even to information stored on hard drives of user workstations.[46]

Individuals with this level of privilege are able to access and alter both the organization's data files and the audit trails that might detect such access; these individuals could also observe communications such as interactive videoconferences without knowledge of the participants. It is worth noting that an individual internal or external to the organization who is successful in intruding on (or, "cracking") a system could acquire the same system-level permissions that are granted to members of the trusted system support staff and then use that power to obtain or modify the organization's data.

As systems professionals, the members of the systems support staff are aware of general principles and organizational restrictions regarding data privacy and security. However, since it is customary for systems support staff to work with the very information that they must prevent others from accessing, and since they are not "clinical professionals," these individuals might not possess the clinical staff's heightened awareness of privacy requirements governing access to patient health information.

Recommendation: Healthcare organizations should implement technical interventions such as a conscientiously applied system audit process and an intrusion detection system that will alert trusted personnel of the occurrence of unauthorized attempts to gain system access (e.g., failed access attempts, inappropriate system and record level data access, anomalous system behaviors, file modifications, etc.). In addition, organizations should ensure that all systems support staff members recognize which system resources are to be accorded the higher level of protection appropriate for PHI and limit the systems support rights to access these system resources to a few trusted and specially trained individuals.

Summary

Many of the recommendations listed above utilize coordinated action in a number of areas to address or reduce potential information vulnerabilities. Table 2 indicates the individual recommendations described in the Executive Summary that are involved in addressing operations/technology issues listed in this section.

[46] While the system support staff's broad access is also granted for their support of the traditional care systems environment, the specialized security and access limitations incorporated into the site's "controlled" clinical information systems reduce their ability to gain undetected access to PHI.

Table 2 - Operations/Technology Recommendations

Recommendation *(see Executive Summary)*	Related Operational/Technical Issue(s)
1 Ensure procedures implemented to protect PHI are compatible across sites	1
2 Implement a strong information privacy culture among the locations that share PHI	1 and 6
3 Ensure only authorized individuals can access telemedicine interactions/information	2, 3, and 6
4 Protect privacy of patient information that is collected via web site interaction	2 (also see Public Policy Issue 3)
5 Select technology based on its ability to protect PHI	3 and 4
6 Implement procedure to control individual users' handling of PHI	3, 4, 5, and 6
7 Ensure communications approaches provide appropriate security for sharing PHI	2, 3, 4, and 5
8 Ensure compatibility of technical measures that sites implement to protect PHI	1 and 5

III. Public Policy Issues and Recommendations

Contributed by Alan S. Goldberg, JD, LLM

Introduction

Similar to providers of traditional in-person care, many organizations and individuals who deliver care using telehealth technologies have in-depth experience in protecting patient privacy. Even before HIPAA requires compliance with its privacy provisions, telehealth providers certified under the Medicare and Medicaid programs have to comply with Conditions of Participation that require many patient privacy protections. *United States vs. Sutherland*[47] evidences a willingness of the court to take account of and give implicit effect to the HIPAA rules in an instance where HIPAA provides guidance, even before the HIPAA enforcement date and in a circumstance that therefore did not afford the court any authority under HIPAA to adjudicate the issue of HIPAA compliance. Here, in adjudicating an objection to requested disclosure of hospital medical records, the court stated, *inter alia*, that "[T]he [HIPAA] Standards indicate a strong federal policy to protect the privacy of patient medical records, and they provide guidance to the present case...." "Although not presently binding on the Hospital or this court, I find these [HIPAA] regulations to be persuasive in that they demonstrate a strong federal policy of protection for patient medical records..." The implication of this judgment is that telemedicine/telehealth providers will have to be aware of possible court proceedings, unrelated directly to HIPAA enforcement, in which a court will nevertheless look to HIPAA for guidance and support in adjudicating issues.

Fortunately, the impact of HIPAA standards and other privacy and security laws might be less burdensome for telehealth providers than other care providers. Because computer technology is a critical component of telehealth care delivery, telehealth providers are likely to be more familiar with privacy and security risks and solutions than other providers. However, if delivery of care using telehealth technologies is not to be encumbered, certain elements of current and proposed policy will require attention and change.

Issues and Recommendations

1 - Telemedicine/telehealth dependence on electronic media means that extensive preparation will be required to comply with the proposed Security Standards

Issue: Unless language of the final Security Standards changes from the proposed wording of the Security Standards, dependence on electronic media will make telehealth interactions subject to stringent requirements on how electronic health information is treated. Since extensive preparation for compliance will be necessary, availability of accurate information is critical to successful compliance.

Recommendation: Encourage HHS to release information promptly on any planned material changes to the proposed Security Standards.

2 - Since any more stringent state law would preempt HIPAA's final Privacy Standards, providers that use telehealth technology could be subjected to inconsistent requirements across their practice areas

Issue: Telehealth practitioners are more likely than other healthcare providers to practice across state lines, thus making them subject to compliance with privacy laws and regulations of each state where they practice. Because many state privacy laws already exist (e.g., in the forms of constitutional law, common law, statutory law,

[47] United States v. Sutherland, Case No. 1:00CR00052, Case No. 1:00CR00093, UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF VIRGINIA, ABINGDON DIVISION, 143 F. Supp. 2d 609; 2001 U.S. Dist. LEXIS 10667, May 1, 2001, Decided.

and administrative law), the provider would have to determine in each situation whether state laws should be considered contrary to and more stringent than HIPAA's Privacy Standards. Providers will face costly operational and many technical complexities in endeavoring to meet differing privacy requirements in each jurisdiction they serve.

Recommendation: To reduce or eliminate the need for each provider to learn and adhere to potentially different privacy laws for each state in which the provider is delivering care, encourage HHS to sponsor a task force to promote harmonization of state and federal laws that deal with privacy of patient information.

3 - Practices of many health-related web sites are not subject to PHI privacy requirements

Issue: A significant volume of "patient information" is acquired through web sites that are not subject to information privacy regulations, even though users might reasonably believe the web sites are health-related. A clash between the desire to have governmental policy protect individual privacy and an aversion to over-regulating the emerging Internet infrastructure is creating a policy and guidance void.

HIPAA Privacy Standards requirements for protecting individuals' medical records and other personal health information apply to organizations that are "covered entities." According to the Office for Civil Rights, "As required by Congress in HIPAA, the Privacy Rule covers health plans, healthcare clearinghouses, and those healthcare providers who conduct certain financial and administrative transactions electronically…The law does not give HHS the authority to regulate other types of private businesses or public agencies through this regulation."[48]

While a great deal of patient information communications on the web is handled by covered entities and therefore protected under HIPAA, there is also a significant volume of information that HIPAA defines as PHI in the possession of organizations that are not covered entities. For example, some web sites collect from individuals information that would be PHI, if HIPAA were applicable, in return for providing information about drugs appropriate for a set of symptoms; similarly, many health-related web sites collect data that would be PHI, if HIPAA were applicable, responding with advice such as disease management protocols or diets.[49]

According to a recent study of the applicability of HIPAA to Internet users, web sites run by HIPAA "covered entities" might include certain components that are not covered by HIPAA protections.[50] Where this is the case, an individual seeking healthcare information or advice might assume that all healthcare information provided is protected by the HIPAA standards even though this is not the case.

Complicating this issue is the fact that, even though the federal government is placing greater emphasis on the individual's right to privacy, the government is showing reluctance to impose

[48] From Frequently Asked Questions in OCR HIPAA Privacy TA 164.000.001 General Overview [*Standards for Privacy of Individually Identifiable Health Information (2000), 45 CFR Parts 160 and 164]*.

(Footnote continues on next page.)

[49] For example: "…for … health-related supplies, the rule applies *only* to those who sell or dispense these items pursuant to a *prescription*. Under this requirement, a pharmacist, such as CVS, is a health care provider, while a Web site that sells books and tapes on losing weight, such as eDiets.com, is not. Similarly, a pharmaceutical company is not a health care provider since it does not sell or dispense drugs pursuant to a prescription." Choy, Hudson, Pritts, & Goldman (2001, p. 13).

[50] For example, purchasing a prescription from a site that accepts only credit cards (and is therefore not a "covered entity" for HIPAA because it does not process health claims in standard format) is outside the scope of regulation, while purchasing the same prescription from a site that takes insurance (e.g., CVS.com or drugstore.com) is protected. Ibid. pp. 7-8, 19-20.

undue regulatory policy and guidance on Internet providers as that technology matures. What must be addressed is clarification of both the government's intent and the boundaries of protection for the PHI an individual shares with an Internet site.

Recommendation: Extend policy to protect PHI wherever it is collected or maintained, including web-based interactions. Either self-regulation or enhancement of existing policy could provide resolution of this issue. For self-regulation, an industry association could develop a set of guidelines closely aligned with the HIPAA Privacy Standards requirements (and any follow-on security regulations for protecting personal information). An organization's adherence to those guidelines or to HIPAA standards could then be acknowledged on each web site that collects PHI so the consumer can make an informed decision on whether to participate based on the privacy policy of the serving organization. If self-regulation does not prove to be an effective solution, then the government should develop policy to provide guidance on information privacy protections to be put in place by any organization or individual that gathers health information about individuals, regardless whether those organizations are practicing medicine or delivering care.

4 - Use of overly specific regulatory language about technical methods for protecting PHI could limit potential for using innovative solutions

Issue: The HIPAA Privacy Standards' general direction to "reasonably safeguard" information and "have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI"[51] allows healthcare organizations to select among approaches that best fit their technical infrastructure. In contrast, language used in the preamble to describe the proposed Security Standards is highly specific, stating, "When using open networks, some form of encryption should be employed."[52] (Note that the wording in the actual proposed standard is somewhat less restrictive, offering "encryption" as an alternative to use of "access controls."[53])

While the proposed Security Standards indicate that "encryption" might or must be applied to protect PHI on "open networks," it is not definitive about the meaning of the term "open network"—making it necessary for covered entities to infer whether an unencrypted transmission is acceptable when sent via radio link (a "safe" open network transmission?) or via an Internet connection (an "unsafe" open network transmission?). A related issue is that the proposed Security Standards' language specifies certain alternative approaches—offering organizations little freedom of choice in selecting among other PHI protection solutions that might become available as newer technologies emerge in the marketplace. (In the encryption example, other forms of protection that might satisfy the objective of protecting the confidentiality of PHI include transmitting only views or data that do not identify the patient, or replacing patient-identifying information with referential identifiers; also, future alternatives might evolve within the communications technologies.)

Recommendation: Following the precedent set in phrasing of the HIPAA Privacy Standards, any

[51] Standards for Privacy of Individually Identifiable Health Information (2000), 45 CFR § 164.530(c)(1) and (2).

[52] Security and Electronic Signature Standards (Proposed Rule) (1998), p. 43255.

[53] The proposed Security Standards state that communications/network control mechanisms must include, among other things: "One of the following implementation features: (A) Access controls (protection of sensitive communications transmissions over open or private networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient). (B) Encryption." Security and Electronic Signature Standards (Proposed Rule) (1998), 45 CFR § 142.308(d), Technical Security Mechanisms.

new policy for protection of information should clearly state the goal (e.g., make PHI undecipherable during communications to anyone other than the intended recipient) and perhaps outline mechanisms for detecting failure to meet that objective, leaving decisions on techniques for achieving compliance to the judgment of organizations subject to the policy.

Summary

The issues described in this section cannot be resolved through actions of individual telemedicine/telehealth participants and organizations. They require that action be initiated by government agencies or through industry-wide consensus. Table 3 indicates the individual recommendations described in the Executive Summary that are involved in addressing policy issues listed in this section.

Table 3 - Policy Recommendations

Recommendation *(see Executive Summary)*	Related Public Policy Issue(s)
9 Release latest plans for HIPAA Security Standards requirements	1
10 Encourage harmonization of state-federal law protecting privacy of patient information	2
11 Extend policy to protect PHI wherever it is collected, including web-based interactions	3 (also see Operational/ Technical Issue 2)
12 Ensure policy statements define goals, permitting affected entities to select techniques	4

IV. Conclusions

No glaring privacy issues or security vulnerabilities preclude or discourage the use of telemedicine/telehealth for delivering care. Since telemedicine practitioners who are cognizant of professional and legal responsibilities to protect the privacy of patient information have typically been the architects of the telemedicine networks they utilize, these individuals have been generally successful in incorporating information protection into their plans. Most information privacy issues relating to use of electronic information and communications technologies to deliver care can be addressed by defining and enforcing effective operational and technical procedure and promoting a strong information privacy culture throughout the organization.

The telemedicine and telehealth activities where the potential information vulnerabilities identified in this study might occur are depicted in Figure 4 as follows: issues described in Section II are shown on the right of the figure; steps of a typical telemedicine interaction (described in Section I) are represented in the columns on the left of the diagram; and check marks indicate where it is possible or likely that the privacy issue could arise during a telemedicine interaction. A summary of this study's recommendations for addressing potential procedural and technical vulnerabilities and enhancing or addressing policy-based issues is provided below.

Operational Practice

Organizations that cooperate to deliver care through use of telehealth technologies must establish a strong culture of confidentiality and a procedural foundation for their shared environment. Many organizations are addressing this as part of their HIPAA preparation activities, using Risk Assessment methodologies to: identify where documented procedures, day-to-day operational practices, and use of technology might create opportunities for information exposure; determine the likelihood of exposure;

Steps of a Telemedicine/ Telehealth Scenario	1.1 OBTAIN PATIENT AGRT./ PERMISSION TO PARTICIPATE	1.2 OBTAIN CONSULTANT AGREEMENT TO PARTICIPATE	1.3 SHARE PATIENT HISTORY WITH CONSULTANT	1.4 SCHEDULE PATIENT VISIT	2.1 REVIEW PATIENT HISTORY	2.2 INITIATE CLINICAL INTERACTION	2.3 INITIATE ENCOUNTER	2.4 DETERMINE DIAGNOSIS/PLAN OF CARE	2.5 PROVIDE FEEDBACK TO PATIENT	2.6 PROVIDE FEEDBACK TO STAFF AT REMOTE SITE/REF. PROVIDER	3.1 DOCUMENT CARE IN PATIENT RECORD	*Issue*
	✔	✔	✔	✔	✔	✔		✔	✔	✔		OI-1 Differences in cooperating locations' operational procedures and technology implementations could cause PHI exposure
						✔			✔	✔		OI-2 Some web sites may not adequately protect the PHI they collect
	✔	✔	✔		✔	✔		✔	✔	✔		OI-3 Care delivery could be observed by unauthorized individuals without patient knowledge or permission
		✔		✔					✔	✔		OI-4 Use of electronic messaging (e.g., e-mail) could expose PHI
						✔		✔				OI-5 Electronic communications could be intercepted by people outside the care delivery domain
	✔	✔	✔	✔		✔		✔	✔	✔		OI-6 Locally stored PHI could be accessed or altered by people with "system-level privileges"

LEGEND: ✔ Step where issue might be encountered

Figure 4 – Telemedicine/Telehealth Interaction Steps Where PHI Exposure Might Occur

and define/implement risk mitigation strategies to reduce the likelihood or consequences of exposure.

Whether the entities involved in conducting telemedicine/telehealth interactions are healthcare organizations or individual providers, and whether these entities are part of a single healthcare organization or distinctly separate business entities, each one must initiate the joint venture by working together to define and implement an effective strategy for information protection. The shared procedure that is developed should define the technical measures that each organization or provider will use to ensure PHI privacy internally at the sites and externally in the shared communications environment; the procedure should also outline steps to be followed by individuals who conduct and support the telemedicine/telehealth delivery of care. Organizations must regularly re-assess operation of their joint venture to ensure that information protection efforts are successful. As either organization considers making procedural or technical changes, both must work together to evaluate the effect of the proposed change on the shared environment and revise procedure as necessary to ensure continuity of the joint information protection capability.

To ensure that all individuals in the organization protect the privacy of patient information, the organizations must establish and maintain a culture of PHI protection. This includes ensuring that members of the non-clinical staff, who do not deal on a regular basis with PHI and might be less aware than clinicians of professional responsibilities to respect its privacy, are made aware of how their job duties relate to PHI. The organizations should maintain a culture of PHI protection through techniques such as including requirements for protecting PHI in all procedure documentation and job descriptions and reminding staff of PHI protection responsibilities through training and periodic re-commitment to PHI confidentiality agreements with the organization. Organizations that contract with outside organizations for services that will deal in some way with PHI should ensure that Business Associate Agreements describe PHI-protection requirements and hold the other organization's staff responsible for maintaining PHI privacy when performing the contracted work.

Organizations that use web site interaction to collect PHI from individuals must incorporate into their operational procedures specific rules for protecting PHI and limiting its use. Web site development and support procedures followed within these organization should be based on the information security "best practice" required by the proposed HIPAA Security Standards and conform to operational characteristics for protecting information privacy that are being generated by various respected healthcare industry professional organizations and trade associations.

Use of Technology

Since healthcare organizations are dependent on technology for effective delivery of care, it is appropriate that they examine and adopt new technologies that might be more efficient, cost-effective, or capability-rich than technologies used in the past. However, it is also necessary that these organizations evaluate how use of the technology might help or hinder PHI protection and define operational procedures that will ensure the technology contributes to protection of PHI.

To reduce unauthorized access to PHI that is saved in a site's technical infrastructure as a result of health-related store & forward and web interactions (e.g., saved in the files of non-clinical application systems, on servers, on workstations, etc.), organizations must implement very specific procedures to be followed by their system users. For example:

- To prevent data access by unauthorized individuals, ensure that information is accessible only by workstations that are under their direct control and only from onsite locations.

- To prevent unauthorized individuals from accessing PHI on the organization's systems, implement user authentication techniques and automatic logoff capabilities.
- To render PHI stored in the organization's infrastructure unintelligible to individuals who are not participants in healthcare electronic information exchanges, require measures such as encryption of messages/documentation that contain PHI before they are saved in the site's repositories or sent offsite.
- To ensure that no e-mail/attachment "residue" is unintentionally left on computers and workstations, implement procedures to purge these items regularly—for instance, each time the user logs off the system.

To reduce the likelihood that communications will be intercepted between sites, organizations and individual providers that participate in telehealth interactions should exercise care in selecting the infrastructure to be employed for information exchange and determine whether special protection is necessary. For example, to ensure protection of information sent across Switched Circuit Networks, consider using applications that are specially designed to protect information that is processed; to protect information sent across Wireless Networks and Packet Networks (e.g., the Internet), consider using the secure Virtual Private Network version of switched circuit network services or consider employing encryption techniques. In general, organizations must ensure that they implement protections that are both appropriate for the care delivery circumstances and technically compatible with the protections implemented at cooperating telehealth/telemedicine sites.

Public Policy

Public policy does not seriously restrict the use of telehealth technologies in either direct provider or indirect consultative healthcare settings. However, there are circumstances where modification of certain policy components, particularly relating to the proposed (as of this writing) HIPAA Security Standards, would reduce the burden of compliance on telemedicine/telehealth providers while continuing to ensure privacy of patients' protected health information.

To reduce the burden of policy that affects telemedicine/telehealth providers to a greater degree than providers using traditional in-person care delivery methods, HHS should:

- Restrict language of the proposed HIPAA Security Standards to describing the goal to be attained—avoiding definition of specific techniques to be applied for meeting the requirement.
- Encourage harmonization of the state and federal laws that deal with privacy of patient information.
- Encourage extension of requirements for protection of data that HIPAA has defined as "PHI" beyond HIPAA's "covered entities" to all organizations (healthcare or non-healthcare) where this type of data is acquired and managed.
- Release information as soon as possible about the currently proposed content of the final Security Standards.

In acting on these recommendations, HHS could reduce the extra burdens currently placed on organizations that are heavily invested in using telehealth technologies and help them to avoid the cost of unnecessary, non-critical activity.

References/Bibliography

Agans, D. A Primer on Video Conferencing Standards. Fletcher Allen Health Care, in Alliance with the University of Vermont. Fletcher Allen Health Care Telemedicine Program. Retrieved April 23, 2001 from: http://www.vtmednet.org./telemedicine/stand.htm.

Anatomy of a Telemedicine Workstation. Office of Telemedicine. University of Virginia Telemedicine Network. Retrieved May 7, 2001 from: http://www.telemed.virginia.edu/about/workstation.htm.

An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. National Institute of Standards and Technology (NIST). Retrieved July 24, 2002 from: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

APA Resource Document on Telepsychiatry Via Videoconferencing. (1998, July). American Psychiatric Association. Retrieved April 11, 2001 from: http://www.psych.org/pract_of_psych/tp_paper.cfm.

Appelbaum, P. (2001, March 22). Testimony of the American Psychiatric Association on the Medical Privacy Regulation before the Subcommittee on Health of the Energy and Commerce Committee, U.S. House of Representatives. American Psychiatric Association. Retrieved April 24, 2001 from: http://www.psych.org/pub_pol_adv/commercehealthtestimony4501.cfm.

ATA Adopts Telehomecare Clinical Guidelines. American Telemedicine Association. Retrieved April 23, 2001 from: http://www.atmeda.org/news/guidelines.html.

"Avoid Standard Un-secure E-mail for Online Communications with Patients," Says Nation's Leading Medical Societies and the AMA, Top Malpractice Carriers and Medem. (2001, April 30). Press Release. Retrieved July 12, 2001 from: http://www.medem.com/Corporate/press/corporate_medeminthenews_press042.cfm.

Beer, K. (August 27, 2001). Secure Messaging Strategies for Healthcare IT Professionals. *ehealth privacy-PSN News*. Retrieved October 24, 2001 from: http://www.privacysecuritynetwork.com/healthnews/symposia/emailstrat.htm.

Berry, Gretchen. (2001, June 4). HIPAA Heads-Up: Keep an Eye on Preemption. *Advance for Health Information Professionals, 11* (11), 20-21.

Binns, K., Zapert, K., & Blythe, B. (2000, October 5). Ethics and the Internet: Consumers vs. Webmasters. Conducted for: Internet Healthcare Coalition and National Mental Health Association (Interview dates: September 6-18, 2000) by Harris Interactive, Inc. Retrieved July 12, 2001 from: http://www.ihealthcoalition.org/content/Harris_report2000.pdf.

Briney, A. (2001, October). 2001 Industry Survey. *Information Security*. 34-46. Retrieved January 2001 from: http://www.infosecuritymag.com/archives2001.shtml#october2001.

Brown-Connolly, N., Monahan, J., & Wood, D. (2000, October 31-November 3). The Blue Cross of California Telemedicine project: A Blueprint for Success. Telehealth 2000 Conference and Exhibition, attendee material.

Chaffee, Mary. (1999, July). A Telehealth Odyssey. *American Journal of Nursing*, *99* (7). Retrieved May 1, 2001 from: http://216.251.241.177/ce/test/article.cfm.

Choy, A., Hudson, Z., Pritts, J., & Goldman, J. (2001, November). Exposed Online: Why the new federal health privacy regulation doesn't offer much protection to Internet users. Washington, D.C.: Pew Internet & American Life Project. Retrieved November 21, 2001 from: http://www.healthprivacy.org/usr_doc/PIP%5FHPP%5FHealthPriv%5Freport%2Epdf.

Crane, L., & Andrews, A. (2002, January 8). Telephone conversation with Bill Schooler and Barbara Clark of the Centers for Medicare and Medicaid Services (CMS), Department of Health and Human Services.

David, Y. (2000, October 31-November 3). International Telemedicine – Issues to Consider. Telehealth 2000 Conference and Exhibition, attendee material.

Dicks, M. (2000, October 31-November 3). HIPAA: Roadsigns and Roadblocks to e-Health. Telehealth 2000 Conference and Exhibition, attendee material.

Dimmick, S., Mustaleski, C., Burgiss, S., & Welsh, T. (2000, February). A Case Study of the Benefits & Potential Savings in Rural Home Telemedicine. *Home Healthcare Nurse, 18* (2), 124-135.

Email Security: Dangerous Waters Ahead. (2001, August). *SC Magazine-Info Security News, 12* (8), 24-30.

eRisk for Providers: Understanding and Mitigating Provider Risk Associated with Online Patient Interaction. (2001, March). Medem, Inc. Retrieved April 11, 2001 from: http://www.medem.com/level2/downloads/eRisk_for_Providers_Mar_01.pdf.

Ferri, C. & Klein, S. (2000, July/August). Telemedicine: New Modalities Complicate the Legal Balance. *MD Computing*, *17* (4), 40-42.

Flowers, C. (2000, October 31-November 3). "An Urban Telehealth Model Program." Telehealth 2000 Conference and Exhibition, attendee material.

Get Patient's Written Consent Before Using E-Mail. (2001). *Health Information Compliance Insider (Sample Issue)*, 5-6.

Gobis, L. An Overview of State Laws and Approaches to Minimize Licensure Barriers. *Telemedicine Today Magazine, 5* (6) *and 6* (1). Retrieved April 25, 2001, from http://www.telemedtoday.com/statelawguide/index.html.

Goldberg, A. (2002, April 29). Internal Report: Telehealth, Privacy, & Health Care: Review, Expectations & Proposals. Goulston & Storrs, Boston, MA.

Goldberg, A. (2002, May 17). Correspondence: Responses to ATI Questions and Comments on ATI Excerpts. Goulston & Storrs, Boston, MA.

Goldman, J. & Hudson, Z. (2000, November/December). Virtually Exposed: Privacy and E-Health. *Health Affairs, 19* (6), 140-148.

Goldman, J., Hudson, Z., & Smith, R. (2000, January). Privacy: Report on the Privacy Policies and Practices of Health Web Sites. Sponsored by the California Healthcare Foundation.

Goldyne, M. (2000, October 31-November 3). Dermatology: The Ideal Clinical Science for Store-and Forward Teleconsultation. Telehealth 2000 Conference and Exhibition, attendee material.

Grove, T. (2002, April 24). Coping with Security of Portable Devices. *HIPAANOTES*, *2* (16) (online newsletter published by Phoenix Health Systems). Available at: http://lyris.dundee.net/cgi-bin/lyris.pl?sub=8513449&id=178578440.

Gue, D. (Ed.) (2001, October 31). The Weakest Link. *HIPAANOTES*, *1* (50) (online newsletter published by Phoenix Health Systems). Available at: http://lyris.dundee.net/cgi-bin/lyris.pl?sub=8513449&id=172177635.

Gue, D. (Ed.) (2002, February 6). The 4 W's and H of HIPAA Security Training. *HIPAANOTES, 2* (5). (Online newsletter published by Phoenix Health Systems). Available at: http://lyris.dundee.net/cgi-bin/lyris.pl?sub=8513449&id=172175226.

Guidelines for Medical and Health Information Sites on the Internet. (2002, May). American Medical Association. Retrieved July 22, 2002 from: http://www.ama-assn.org/ama/pub/printcat/1905.html.

Guidelines for Online Communications and Consultations. (2001, November). Medem, Inc. Retrieved April 11, 2001 from: http://www.medem.com/corporate/corporate_erisk_guidelines.cfm.

Guidelines for Physician-Patient Electronic Communications. (2001, June). American Medical Association. Retrieved July 12, 2001 from: http://www.ama-assn.org/ama/pub/category/2386.html.

HCFA Internet Security Policy. (1998, November 24). Retrieved July 12, 2001 from: http://www.hcfa.gov/security/isecplcy.htm.

Health Web Site Standards, Version 1.0. (2001). URAC. Retrieved September 14, 2001 from http://websiteaccreditation. urac.org/.

HIPAA Notice of Privacy Practices—Preliminary Draft. (2001, November). American Medical Association. Retrieved August 21, 2002 from: http://www.ama-assn.org/ama/pub/category/6699.html.

Home Network Security. CERT© Coordination Center. Retrieved July 12, 2001 from: http://www.cert.org/tech_tips/home_networks.html#11-D.

How to Schedule a Patient. Missouri Telehealth Network. Retrieved April 2, 2002 from http://www.muhealth.org/~telehealth/clinserv/howtoschedule.html.

Hutson, J., (1999, Winter). Managing Telehealthcare Information. *Journal of the Healthcare Information and Management Systems Society*, *13* (4). Retrieved September 5, 2000, from: http://www.himss.org/members/secure/journal/13-4/13406.html.

Igras, E., Bergman, D., Ulmer, R., & Sargious, P. (2000, May 21-24). Guidelines for the Implementation of *Interoperable* Telehealth Networks. American Telemedicine Association Conference, attendee material.

Kane, B., & Sands, D. (1998, Jan/Feb). Guidelines for the Clinical Use of Electronic Mail with Patients. Reprinted from the *Journal of the American Medical Informatics Association, 5* (1), Retrieved March 7, 2001 from: http://www.amia.org/pubs/other/email_guidelines.html.

Kumekawa, J. (2001, August). Health Information Privacy Protection: Crisis or Common Sense. (pre-publication copy).

Kumekawa, J. (2001, February 18). The New HIPAA Privacy Rules: What Do Telemedicine Practitioners Need to Know? Retrieved April 25, 2001 from: http://telehealth.hrsa.gov/pubs/privac.htm#report.

Levy-Biehl, H. (2000, November 3). Security and Privacy in the eHealthcare Age. Telehealth 2000 Conference and Exhibition. Presentation provided via e-mail to the author.

Lovata, F. (2000, May 21-24). Telemedicine via the Internet: Successful Program Strategies. American Telemedicine Association Conference, attendee material.

Lumpkin, J. (2000, November/December). E-Health, HIPAA, and Beyond. *Health Affairs*, *19* (6), 149-150.

Mayor, T., & Bass, A. (2001, January 15). The Privacy Problem: Health Care. *CIO*, pp. 75-84.

McClure, S., & Scambray, J. (2000, May 26). Switched networks lose their security advantage due to packet-capturing tool. Retrieved October 24, 2001 from: http://www2.infoworld.com/articles/op/xml/00/05/29/000529opswatch.

Model Guidelines for the Appropriate Use of the Internet in Medical Practice. (2002, April). Report of the Special Committee on Professional Conduct and Ethics. Federation of State Medical Boards. Available from: http://www.fsmb.org/ (follow link to "Policy Documents").

Mossy, G. (2000, December 3). Securing a Medical Information System at a Federal Research Agency. SANS Institute Information Security Reading Room. Retrieved January 16, 2001 from: http://www.sans.org/infosecFAQ/securitybasics/med_info.htm.

Murphy, G. (Chair of HealthKey Privacy Advisory Group). (2001, May 15). A Framework and Structured Process for Developing Responsible Privacy Practices. (Report for the HealthKey Program/The Robert Wood Johnson Foundation.)

O'Harrow, R. (2001, July 4). Prozac Maker Reveals Patient E-Mail Addresses. *The Washington Post*. Retrieved July 10, 2001 from: http://www.washingtonpost.com/wp-dyn/articles/A16718-2001Jul4.html.

OCR HIPAA Privacy TA 164.000.001 General Overview. (2001). Office for Civil Rights. Retrieved November 28, 2001 from: http://www.hhs.gov/ocr/hipaa/genoverview.html.

Overview of the eRisk in Healthcare Project of the eRisk Working Group for Healthcare and eRisk Sample Policies and Disclaimers. (2001, November 1). Retrieved April 11, 2001 from: http://www.medem.com/level2/downloads/eRisk_Overview_v2.pdf and http://www.medem.com/level2/downloads/eRisk_Sample_Policies_and_Disclaimers_v1.pdf.

Pappas, D. (2001, Winter). New Technique Finds Lost Data. *NIST Research for Industry: Technology at a Glance*, 3-4.

Piller, C. (2001, November 7). Web Mishap: Kids' Psychological Files Posted. *Los Angeles Times.* Retrieved November 15, 2001 from: http://www.latimes.com/news/nationworld/nation/la-110701private.story.

Practice Brief: E-mail Security (Updated). (2000, February). American Health Information Management Association. Retrieved April 9, 2001 from: http://www.ahima.org/journal/pb/00.02.html.

Pritts, J., Goldman, J., Hudson, Z., Berenson, A., & Hadley, E. (1999, August 8). The State of Health Privacy: An Uneven Terrain (A Comprehensive Survey of State Health Privacy Statutes). Available from: http://www.georgetown.edu/research/ihcrp/privacy/statereport.pdf.

Puskin, D. & Kumekawa, J., eds. (2001, January). *2001 Telemedicine Report to Congress*, U.S. Department of Health and Human Services.

Puskin, D., Mintzer, C., & Wasem, C. (1997). Chapter 14, Telemedicine: Building Rural Systems for Today and Tomorrow. In P. Brennan, S. Schneider, & E. Tornquist (Eds.), *Information Networks for Community Health.* (p. 276). Computers in Health Care Series. Springer-Verlag.

Radcliff, D. (2001, September 17). Secrets In the Air. *Computerworld*. Retrieved October 3, 2001 from: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63887,00.html.

Radding, A. (2001, January 1). Crossing the Wireless Security Gap. *Computerworld.* Retrieved October 17, 2001 from: http://computerworld.com/cwi/story/0,1199,NAV65-663_STO55583_NLTS,00.html.

Rich, J. & Edelstein, S. E-Health and Oncology: A Legal Perspective. (2001). *Oncology Issues, 16* (6), 15-17. Retrieved on July 30, 2002 from: //http://www.medscape.com/viewarticle/421479.

Rosen, E. Twenty Minutes in the Life of a Tele-Home Health Nurse. *Telemedicine Today Magazine.* Retrieved April 25, 2001 from: http://www.telemedtoday.com/articlearchive/articles/Telehomenurse.htm.

Salkever, A. (2001, September 11). Wireless Networks: Open Doors for Bad Guys. *Business Week Online.* Retrieved January 24, 2002 from: http://www.businessweek.com:/print/bwdaily/dnflash/sep2001/nf20010911_0545.htm.

Sands, D. (1999). Guidelines for the Use of Patient-Centered E-mail. Massachusetts Health Data Consortium. Retrieved July 12, 2001 from: http://www.mahealthdata.org.

Sato, D. (2000, October 31-November 3). Telemedicine Implementation and Application Strategies in a Public Hospital System. Telehealth 2000 Conference and Exhibition, attendee material.

Security and Electronic Signature Standards (Proposed Rule). (August 12, 1998). Title 45 Code of Federal Regulations Part 142. *Federal Register, 63* (155), 43241. Available at: http://aspe.hhs.gov/admnsimp/nprm/seclist.htm.

Selecting a Video Encryption System. (2001). Retrieved October 22, 2001 from: http://www.ovation.co.uk/VielockII/SELECT.HTM.

Stamm, B. (1998). Clinical Applications of Telehealth in Mental Health Care. American Psychiatric Association. Retrieved December 11, 2001 from: http://www.apa.org/journals/pro/pro296536.html.

Standards for Privacy of Individually Identifiable Health Information. (December 28, 2000). Title 45 Code of Federal Regulations Parts 160 and 164, *Federal Register*, *65* (250), 82461. Final Rule. (August 14, 2002). *Federal Register, 67* (157), 53182. Available at: http://www.hhs.gov/ocr/hipaa/finalreg.html.

Stepanek, M. (2000, December 11). Who's Prying Now? *Business Week*, 80.

Swanson, M. and Guttman, B. (1996, September). Generally Accepted Principles and Practices for Securing Information Technology Systems. National Institute of Standards and Technology (NIST). Retrieved July 24, 2002 from: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Szabo, D. (2001, June 6). Implications of HIPAA Privacy Regs for Webmasters / Intake of Personally Identifiable health Information Via the Web. Massachusetts Health Data Consortium Webmaster Group Meeting, Massachusetts Health Data Consortium. Retrieved July 12, 2001 from: http://www.mahealthdata.org.

Tabar, P. (2002, January). You've got mail. Plus problems? and Don't Forget the Mail Server. *Healthcare Informatics*. Retrieved February 26, 2002, from: http://www.healthcare-informatics.com/issues/2002/01_02/trends.htm.

Telecommunications: Protecting the Forgotten Frontier. (2001, August). *SC Magazine-Info Security News*, *12* (8), 36-40.

Terry, K. (September 3, 2001). E-mail patients? Don't be nervous. Do be careful. *Medical Economics*. Retrieved October 24, 2001 from: http://me.pdr.net/me/public.htm?path=content/journals/m/data/2001/0903/emailrisks.html .

The Practice of Internet Counseling. National Board for Certified Counselors, Inc. and Center for Credentialing and Education, Inc. (2001, November 3). Retrieved July 22, 2002 from: http://www.nbcc.org/ethics/webethics.htm.

Treese, W. (2000, June). Going Wireless. *NetWorker, 4* (2), 9-12.

United States General Accounting Office. (2001, April). Medical Privacy Regulation: Questions Remain About Implementing the New Consent Requirement. (Report to the Chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate). Washington, DC: U.S. Government Printing Office.

Verton, D. & Brewin, B. (2001, August 13). Potentially Dangerous Wireless LAN Threats Discovered. *Computerworld*. Retrieved August 15, 2001 from: http://www.computerworld.com/rckey68/story/0,1199,NAV63_STO63026,00.html.

Vijayan, J. (2002, May 24). Business partners, third parties can pose security risk. *Computerworld*. Retrieved May 29, 2002 from: http://computerworld.com/securitytopics/security/cybercrime/story/0%2C10801%2C71459%2C00.html?nlid=EB.

Waters, R., & Spencer, A. (2001, August 9). Internal Report: Applicability of HIPAA Regulations to Telemedicine Operational Scenarios. Arent Fox, Washington, D.C.

Who Is The Joint Commission on Accreditation of Healthcare Organizations? Joint Commission on Accreditation of Healthcare Organizations (JCAHO). Retrieved August 27, 2002, from: http://www.jcaho.org/general+public/who+jc/who+is+the+joint+commission.htm.

Who Knows your Medical Secrets? (2000, August). *Consumer Reports*, 22-26.

Worthen, B. Communication Tools-Making Connections. *CIO.com Online Newsletter*. Retrieved November 6, 2001 from: http://www.cio.com/online/110601_telcon.html.

Appendix

A – Overview of HIPAA

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the most significant body of healthcare legislation to be enacted since Medicare. It was signed into effect to protect health insurance coverage for workers and their families when they change or lose their jobs (Portability) and to protect health data integrity, confidentiality, and availability (Accountability). HIPAA consists of Titles I-V and places various legal requirements and financial penalties on the healthcare industry. Of the five Titles, Title II is the most germane to this report.

Title II -- Administrative Simplification

Title II contains the provisions that pose the greatest challenge to healthcare organizations today and will have the biggest impact on business partners exchanging electronic transaction data, specifically: Preventing Healthcare Fraud and Abuse, Administrative Simplification, and Medical Liability Reform. Every link in the electronic communication chain is affected, including providers and benefits payers that exchange claim and payment data. Processes that are affected by HIPAA include enrollments and eligibility transactions, provider transactions and communications, claim transactions, and remittance advice. Title II:

- Mandates the format and content of electronic transactions that are passed between health insurers and other entities, collectively known as trading partners; and
- Addresses provisions related to patient confidentiality and privacy and electronic signature.

The goal of Administrative Simplification is to reduce the costs and administrative burdens of healthcare through standardization and improved security standards. The provisions establish various protections, standards, and requirements for the transmission, storage, and handling of electronic healthcare transactions. The privacy protections extend to personal health information that is not electronic, such as medical record files.

The Administrative Simplification provisions adopt standards for privacy, security, electronic signatures, unique identifiers, and electronic healthcare transactions. These standards in the provision are designed to:

- **Standardize the interchange of electronic data for specified administrative and financial transactions.**
  The new regulations are an effort to reduce paper work and increase efficiency and accuracy through the use of standardized financial and administrative transactions and data elements for transactions. HIPAA will change this practice by requiring payers to accept certain specified transaction standards for EDI.

- **Protect the security and confidentiality of electronic health information.**
  The privacy regulations grant healthcare consumers a greater level of control over the use and disclosure of personally identifiable health information. In general, healthcare organizations are prohibited from using or disclosing health information except as

authorized by the patient or specifically permitted by the regulation. The privacy rule applies to all personally identifiable health information, irrespective of form; there is no exclusion for written medical records or oral communications. The regulations are applicable to all health information held or created by the covered entity.

Implications

HIPAA is an enterprise-wide issue, not simply an information technology issue. Legal, regulatory, process, security, and technology aspects of each component of the legislation must be carefully evaluated before an organization can begin its implementation plan. The requirements outlined by the law and the regulations promulgated by the Department of Health and Human Services are far-reaching—all health plans, healthcare clearinghouses, and healthcare providers, from large integrated delivery networks to individual physician offices must comply.

B – Abbreviations and Acronyms

AMA	American Medical Association
CMS	The Centers for Medicare and Medicaid Services
COPPA	Children's Online Privacy Protection Act
CP	Consulting Provider
CPR	Computerized Patient Record
CPS	Consulting Provider Staff
HHS	Department of Health and Human Services
HH	Home Health
HIPAA	Health Insurance Portability and Accountability Act of 1996
IP	Internet Protocol
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
NPP	Notice of Privacy Practices
NPRM	Notice of Proposed Rule Making
OAT	Office for the Advancement of Telehealth
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PC	Personal Computer
PHI	Protected Health Information
Privacy Standards	HIPAA Standards for Privacy of Individually Identifiable Health Information
RP	Referring Provider
RPS	Referring Provider Staff
Security Standards	HIPAA Security and Electronic Signature Standards (Proposed Rule)
SSL	Secure Socket Layer
TEMP, TEMPorary, TMP	Temporary (as in temporary storage locations of a personal computer or workstation)
URAC	American Accreditation HealthCare Commission
VPN	Virtual Private Network