HEALTHCARE PERSPECTIVE

ISSUE 14

CNA We can show you more.®

nso®

HPSO®

Telemedicine: Risk Management Issues, Strategies and Resources

Telemedicine is the practice of electronically connecting geographically discrete healthcare facilities and providers. It encompasses numerous methods and technologies, ranging from traditional store-and-forward data applications, commonly utilized in diagnostic review and interactive exams, to innovative "telepresent" methods, including robotic surgery and emergency services consultations.* Among other uses, telemedicine applications permit:

- **Patients/clients in underserved rural areas** to enjoy improved access to quality care, and state-of-the-art settings.
- **Practitioner networks** to collaborate via shared electronic medical records, digital imagery and data files.
- **Specialty providers** to communicate with (or "tele-assist") primary care practitioners in diagnostic tasks, leading to enhanced outcomes, shorter treatment periods, decreased use of unnecessary drugs and reduced costs.
- **Emergency department personnel** to video-link with trauma specialists for instant access to life-saving information and support.

While telemedicine/telehealth (TMH) can foster efficiency and convenience, its reliance on continuous, real-time transmission of data over computer networks also creates risk. At every step of the process, adverse events may occur, including diagnostic errors, technical glitches, and patient/client privacy and security violations.

This edition of *Healthcare Perspective* outlines strategies designed to enhance clinical, operational and technical processes associated with the provision of TMH. National standards are cited throughout this resource, serving as policy templates in the following key areas: network security, confidentiality, quality improvement, informed consent, record maintenance and technical support. The readiness self-assessment tool on pages 7-9 is designed to aid organizations in creating a sound TMH program or measuring compliance with existing parameters.

SECURITY: Safeguard patient/client data on computer networks and during transmission.

Secure transmission of clinical information requires effective safeguards at every point in the process, i.e., within the transmitting facility's network, over the transmission medium and at the distant site. Whether data are sent by satellite, through the Internet or over a virtual private network (VPN), the following security measures, among others, should be established and implemented:

Authentication enables authorized users to enter the system and access data via such means as log-in passwords, biometric scans, voice pattern samples and smart cards. Authentication procedures also permit system administrators to verify specific users and their means of interface. Outside access should be limited to those networks that fulfill organizational security requirements.

Patient/client identification uses patient/client integration profiles to promote accurate verification at multiple sites. These profiles enable the cross-referencing of patient/client identifiers either from multiple domains or from a central patient/client information server.

Data control ensures that patient/client information is stored and transmitted in a confidential manner through the creation of a VPN, use of encryption technology and/or file anonymization software. An increasing number of medical systems also require digital signatures to verify that data have not been modified by an unauthorized user. Encryption measures also should extend to stored data on portable devices or removable media, as theft and loss of laptops, tablets, smartphones, discs and USB flash drives are a leading source of data breaches.

Data tracking offers an audit trail of all exchanges involving medical information, permitting the system administrator to verify who has used the system and/or accessed patient/client data. Related monitoring technologies help identify and protect against technical glitches and hacking.

Protected access systems safeguard telemedicine applications on wireless networks. A variety of security mechanisms may be used to provide both logical and physical restrictions, including firewalls and antivirus software that detects malicious programs and activity.

* For a list of additional healthcare applications in telemedicine, see Winter, R. "9 Killer Telemedicine Apps That Will Revolutionize Healthcare," from Soliant Healthcare, July 21, 2009.

PATIENT/CLIENT CONFIDENTIALITY: Draft a disclosure protocol to ensure compliance with privacy regulations.

Privacy is a paramount concern when transmitting electronic data. Unauthorized network access, hardware tampering and interception of data may violate privacy requirements imposed under HIPAA, as well as other governing federal and state laws and regulations. Both TMH partners should implement a disclosure protocol incorporating the following practices:

- **Obtain written permission from the patient/client** before transmitting any protected health information.
- **Require all staff involved in TMH to execute confidentiality agreements,** including contract and vendor personnel.
- **Allow only designated professionals to disclose health related information,** such as the telepresenter and consulting and referring practitioners.
- **Mandate HIPAA training for staff and providers,** covering such topics as information security, common sources of breaches and consequences of protocol noncompliance.
- **Transmit patient/client data on an as-needed basis** and monitor staff for inappropriate access to protected health information.

The privacy obligations of healthcare practitioners extend to the environment where interactive consultations occur. The following provisions can help safeguard patient confidentiality:

- **Ensure that the patient/client is aware of and grants approval for all personnel participating in consultations,** including the telepresenter.
- **Place a conspicuous sign on the exam door,** notifying others that a consultation is in progress.
- **Prohibit the use of unauthorized cameras and cellular telephones in the examination room,** using a signed consent agreement if necessary.
- **Schedule TMH sessions in a designated area that is suitably enclosed and private,** rather than in an administrative suite or other public space.

QUALITY IMPROVEMENT: Measure outcomes for clinical care and technical support.

Delivery of high-quality TMH services depends upon systematic monitoring and ongoing improvement of key processes. The following basic measures can help business owners more effectively compile, evaluate and report on meaningful care-related data.

Outcome measurement offers practitioners useful information about how well a TMH program is functioning, including further refinements that may be needed. Indicators should capture clinical, efficiency and satisfaction outcomes, including:

- Patient/client complication and morbidity rates.
- Compliance with provider performance criteria.
- Diagnostic accuracy.
- Adherence to clinical protocols.
- Referral rates.
- Patient/client satisfaction levels.
- Cost per case.
- Delays in accessing consultations, referrals or specialty providers.
- Average waiting times.

Standardized clinical protocols, properly implemented, can enhance quality and efficiency. By outlining a step-by-step process, protocols help improve consistency of care and performance of staff, and also ensure that test results are delivered in a timely, accurate and confidential manner. For interactive consultations, protocols minimally should advise providers on how and when to:

- Schedule a consultation.
- Arrange for a consulting room.
- Set up necessary equipment.
- Establish network connections.
- Prepare and advise the consulting provider, patient/client and telemedical presenter.
- Document consultation findings.
- Secure and back up required data.
- Prepare reports.
- Inform patients/clients and other providers of test results.

The American Telemedicine Association has promulgated a variety of practice guidelines. In addition, the Telehealth Resource Center provides information on protocol development.

Incident reporting helps providers identify and respond to patient/client complications or other adverse events that may arise during telemedicine care. Providers should be instructed to document occurrences and forward reports promptly to the appropriate individual per written policy. A thorough, timely review of events helps foster a culture of accountability and continuous improvement.

Regular equipment testing and maintenance helps prevent potential technical and user problems. Equipment should be suitable for diagnostic and treatment uses, readily available when needed and fully functional during clinical encounters. Safety guidelines should specify who is responsible for maintenance. Utilize checklists or logs to facilitate documentation of post-installation testing, pre-session calibration, and ongoing quality checking of audio, video and data transmission capabilities.

Satisfaction surveys capture vital data regarding patient/clients and provider perceptions of the TMH program, as well as utilization patterns and the overall quality of TMH care. Surveys also can reveal unexpected barriers to care, including accessibility issues and cost. Sample survey formats for telehealth encounters are available here and here.

TRAINING: Employ interactive teaching modules to ensure key competencies.

Staff training should focus primarily on learning the skills necessary to conduct consultations and other TMH services smoothly and efficiently. At a minimum, training sessions should aim to enhance the following competencies:

- **Communication skills,** including video presentation content, organization and etiquette.
- **Understanding the scope of services** that can be provided using TMH methods.
- **Proficiency with the technology system in use,** as well as the physical environment.
- **Knowledge of operational protocols and procedures,** updated as necessary.
- **Ability to respond to equipment malfunctions** and manage unexpected occurrences.

Optimally, staff should begin with separate training sessions at the originating and distant sites, then progress to mock joint procedures before advancing to real-time provision of care. A wide variety of training modules is available, serving a range of procedures and existing proficiency levels. The Telehealth Resource Center offers guidance on developing a training strategy, as well as answers to commonly asked questions concerning training of TMH providers.

INFORMED CONSENT: Disclose risks unique to the practice of telemedicine.

Patient/client consent is always required prior to participation in TMH services. Providers often use existing consent and documentation processes for store-and-forward consultations. For more invasive procedures, a separate consent form is preferable, encompassing the following information:

- Names, credentials, organizational affiliations and locations of the various health professionals involved.
- Name and description of the recommended procedure.
- Potential benefits and risks.
- Possible alternatives, including no treatment.
- Contingency plans in the event of a problem during the procedure.
- Explanation of how care is to be documented and accessed.
- Security, privacy and confidentiality measures to be employed.
- Names of those responsible for ongoing care.
- Risks of declining the treatment/service.
- Reiteration of the right to revoke consent or refuse treatment at any time.

In addition, clearly convey to the patient/client the inherent technical and operational hazards that may impede communication with the distant site or otherwise prevent prompt, accurate diagnosis of patient/client conditions. These include:

- **Fiber-optic line damage, satellite system compromise or hardware failure,** which could lead to incomplete or failed transmission.
- **File corruption during the transmission process,** resulting in less than complete, clear or accurate reception of information or images.
- **Unauthorized third-party access,** which may lead to data integrity problems.
- **Natural disasters,** such as hurricanes, tornadoes and floods, which can potentially interrupt operations and compromise computer networks

Consent form documentation becomes part of the patient/client healthcare information record and is customarily maintained at the originating site, where the patient/client receives routine care. Sample telemedicine informed consent forms are available from the American Telemedicine Association.

Glossary of Telemedicine/Telehealth Terminology

The following terms appear frequently in national standards, practice guidelines and clinical policies relating to telemedicine and telehealth.

- **Asynchronous transmission:** One-way rather than simultaneous mutual communication of medical images or information, as utilized in store-and-forward encounters.
- **Authentication:** A method of verifying the identity of a person sending or receiving information, using passwords, "keys" or other unique label identifiers.
- **Distant site:** Physical location of a provider/specialist who is remotely seeing a patient/client or consulting with another provider. The site also referred to as consulting, hub, specialty, provider or referral site.
- **Encryption:** A system of encoding electronic data so that information can be retrieved and decoded only by the individual or computer system authorized to access it.
- **Internet protocol:** A connectionless protocol by which data is sent from one computer to another over the Internet. Each computer has at least one address that uniquely identifies it from all other computers on the Internet.
- **Interoperability:** The ability of two or more systems (e.g., computers, communication devices, networks, software or other information technology components) to interact with each other and exchange data.
- **Originating site:** The physical location of a patient/client and/or the practitioner of the patient/client during a telehealth encounter or consult. Also referred to as patient/client, remote, rural or spoke site.
- **Store-and-forward:** A type of telehealth encounter or consultation using still digital images of patient/client data for the purpose of rendering a medical opinion or diagnosis. The technique is most commonly used in the fields of radiology, pathology, dermatology, home health and wound care.
- **Synchronous transmission:** Two-way, simultaneous electronic exchange of information, as utilized in interactive video sessions.
- **Telemedicine and Telehealth:** Telemedicine is the use of medical information exchanged from one site to another via electronic communications to improve patients' health status. Closely associated with telemedicine is the term "telehealth," which is often used to encompass a broader definition of remote healthcare that does not always involve clinical services. Videoconferencing, transmission of still images, e-health including patient portals, remote monitoring of vital signs, continuing medical education and nursing call centers are all considered part of telemedicine and telehealth. Telemedicine is not a separate medical specialty.
- **Telepresence:** The use of a set of technologies, generally inclusive of high-definition quality audio/video, that allows providers to perform procedures remotely while receiving sensory information or other feedback, producing a sense of being in attendance at the remote site. Also refers to the use of robotic or other related medical instruments to perform procedures remotely by manipulating devices while also receiving sensory information or other feedback, producing a sense of being in attendance at the remote site.
- **Telepresenter:** A healthcare practitioner or other individual at the originating site who is trained in the use of telehealth technology and is responsible for assisting the patient/client, managing the equipment and performing other hands-on activities during the examination.
- **Virtual private network:** A method to carry private communications over the public Internet using tunneling or port forwarding, which is the transmission of private data over public lines in an encapsulated form.

Source: The American Telemedicine Association.

RECORD MAINTENANCE: Create and retain formal patient/client care records for all TMH encounters.

Telemedicine sessions should be as thoroughly documented as all other patient/client encounters, with both partners to the TMH agreement contributing to the process. According to the American Health Information Management Association, TMH records minimally should include:

- Patient/client name.
- Patient/client identification number at originating site.
- Date of service.
- Referring practitioner's name.
- Consulting practitioner's name.
- Provider organization's name.
- Type of evaluation to be performed.
- Informed consent documentation.
- Evaluation results.
- Diagnosis/impression of providers.
- Recommendations for further treatment.

The use of standardized intake and consultation forms can help providers achieve compliance with documentation parameters. Templates, such as those available from the American Telemedicine Association, offer staff a clear and consistent documentation format for evaluations and consultations.

Facilities also must select acceptable media for record keeping, such as electronic files, hard copy, and/or video or audiotape. Protocol routinely dictates that the originating site retains files and images, providing the distant site with access to data when needed. Record retention policies should comply with professional standards, federal and state laws and regulations, and the reimbursement requirements of public and private payers.

Healthcare business owners can help streamline the archiving process by assigning "lifespans" to patient/client data and medical documents stored in computer memories, based on such factors as last date of patient/client treatment, provider access requirements and record retention policies. For many organizations, data are maintained on a locally designated and protected server, with replication servers backing up files in the event of a disaster, computer problem or other type of business interruption.

TECHNICAL SUPPORT: Implement a robust, high quality telecommunication system.

Interactive TMH encounters depend upon a reliable and secure telecommunication system. Connections are of the utmost importance and should support business-grade videoconferencing with clear sound. Available options range from portable video conferencing units to large screen, high-definition consoles. Relying on the basic Internet for connection, rather than a private network dedicated to healthcare applications, may compromise quality and interfere with effective diagnosis or treatment.

Healthcare business owners can streamline the equipment selection process by compiling a list of general requirements and technical specifications for videoconferencing systems, ancillary devices and post-purchase support needs. Choices are generally guided by imaging needs, existing infrastructure and budgetary realities. Regardless of the specific equipment selected, TMH systems should:

- **Comply with all relevant laws,** regulations and codes regarding patient/client safety and technical requirements.
- **Provide redundant systems** to help ensure uninterrupted network connectivity.
- **Utilize connections exclusively designated for telemedicine,** rather than local networks, which may be incompatible with TMH image transmission and archiving applications, and/or lack sufficient bandwidth.
- **Permit networks to connect** through existing firewalls.

It also is necessary to accommodate the physical and environmental demands of TMH operations. Patient/client rooms must be sufficiently spacious to allow at least six feet between the patient/client and the camera operator. In addition, adequate HVAC capabilities and accessible infection control supplies – such as antibacterial wipes, sterile plastic sleeves for probes and camera lens disinfectant are essential to patient/client safety.

As with any new venture, successful implementation of a telemedicine program requires careful planning and collaboration by multiple stakeholders, both inside and outside the business. The strategies presented in this resource can help healthcare business owners initiate and maintain a high quality TMH program, which maximizes efficiency and convenience while minimizing associated risks.

Telemedicine Regulations: Frequently Asked Questions

As the reach of telemedicine services expands, questions arise regarding the permitted scope of practice, licensure requirements and HIPAA compliance, among other regulatory-based inquiries. The questions and responses below provide basic information to practitioners and are intended to serve as a catalyst for further inquiry into the federal and state regulatory framework for telemedicine/telehealth (TMH).

WHAT QUALIFIES AS TMH?

TMH involves the use of electronic communications and information technology to deliver health-related services at a distance, typically in real time. States have different laws concerning when and how TMH may be practiced, so it's important to check state statutes, regulations and policies, as well as state licensure boards regarding practice limitations before initiating services. In addition, the Centers for Medicare & Medicaid Services provide information on the scope of Medicare telehealth services.

WHO CAN PROVIDE CARE VIA TMH?

It is essential to verify with the relevant state professional licensing board the practitioners who can legally practice TMH. Depending on the state, authorized practitioners may include physicians, clinical nurse specialists, nurse practitioners, physician assistants and licensed counselors and therapists, among others.

IS A PATIENT/CLIENT RELATIONSHIP ESTABLISHED WITH TMH?

A patient/client provider relationship is established via TMH in the same manner in which it is established in an in-person office/hospital setting.

IS IT NECESSARY TO SECURE A LICENSE IN BOTH STATES WHEN DELIVERING TMH ACROSS STATE LINES?

Some states require practitioners who practice TMH to be licensed in the state where the patient/client is located, and abide by the licensure and practice requirements of that state. Before embarking on interstate TMH, practitioners must review the state practice act of the state where the patient/client resides. If a state practice act is silent regarding TMH, or published opinions or interpretations regarding the subject of licensure have not been issued by recognized sources, then potential TMH practitioners should contact their state professional licensing board for clarification with respect to interstate practice and their licensure status. Certain states also have entered into interstate compacts, creating a new pathway to expedite the licensing of a practitioner seeking to practice in multiple states. For additional information, check the respective state licensing board to determine if the state has joined a compact.

SHOULD A SPECIAL CONSENT-TO-TREAT FORM BE UTILIZED WHEN PERFORMING TMH?

Obtaining a patient's/client's consent to TMH services is an essential step in the care process, and is a recommended best practice of the American Telemedicine Association. A general consent-to-treat form lacks specificity regarding the potential benefits, constraints and risks unique to TMH, including equipment failures and privacy and security breaches. In addition, a general form is lacking in standard language regarding patient/client rights and responsibilities relating to TMH. See section "Informed Consent: Disclose Risks Unique to the Practice of Telemedicine" for a link to sample TMH consent forms.

DOES A PRACTITIONER NEED TO ABIDE BY HIPAA REGULATIONS?

TMH services must comply with the same HIPAA-related rules and regulations at the federal and state levels, as well as business policies, that apply to the delivery of in-person services. Practitioners should be conversant with the HIPAA Breach Notification Rule and technology encryption requirements. In the case of interstate practice, if requirements for privacy, security and informed consent differ between states, practitioners are encouraged to follow the most restrictive laws and regulations.

Telemedicine Readiness Assessment Tool

The following risk control recommendations are designed to serve as a starting point for healthcare business owners seeking to assess and enhance their risk control practices in the area of telemedicine/telehealth (TMH). For additional risk control tools and information, visit www.cna.com/healthcare, www.nso.com and www.hpso.com.

RISK CONTROL MEASURES	STATUS	COMMENT/ ACTIONS PLAN
PROGRAM MISSION AND BUSINESS CONSIDERATIONS		
Organizational leadership visibly supports a TMH program and spearheads development efforts.		
The TMH leadership team has created a written business and operational plan regarding the provision of TMH services, including:		
- A cost, benefit and risk analysis, along with marketing, communication and assessment strategies.		
- Human and financial resources available for implementation.		
- An estimate of when the program will become self-sustaining.		
The plan includes goals for the TMH program, as well as models for interdisciplinary and inter-organizational cooperation.		
Potential TMH partners are identified and scrupulously evaluated in terms of clinical, technical and cultural affinity.		
A business associate agreement is signed with all TMH partners, pursuant to HIPAA requirements.		
A memorandum of agreement, reviewed by legal counsel, articulates responsibilities for originating and partner sites, providing specific answers to the following key questions, among others:		
- Who provides support staff?		
- Who pays for telecommunication connections?		
- Who supplies and supports equipment?		
- What space is available for telemedicine procedures?		
- Who manages the billing process?		
ORGANIZATIONAL READINESS		
A TMH working committee is established and maintains ongoing communication with relevant stakeholders.		
A designated TMH coordinator is named and charged with providing support for referrals, clinical decisions, program functioning and system processes.		
A written TMH procedure manual is issued, which conforms to practice guidelines of nationally recognized associations.		
TMH-related roles and responsibilities are clearly defined, encompassing different medical disciplines and staff levels.		
TMH credentialing, privileging and medical peer review processes are delineated, addressing patient/client safety, jurisdictional and liability considerations.		
A consistent referral and scheduling system is established, which is clear, detailed and easy to use.		
TMH procedures are regularly evaluated to ensure compliance with patient/client protection laws, including applicable HIPAA, OSHA and CDC, and state laws and regulations.		

RISK CONTROL MEASURES	STATUS	COMMENT/ ACTIONS PLAN
TRAINING REQUIREMENTS		
Educational and professional development requirements are specified, including equipment training, participation in pilot programs and familiarity with clinical protocols.		
Ongoing training – including review of proper documentation practices – is required for continued participation in the TMH program.		
Staff are trained in incident reporting, and adverse TMH occurrences are tracked and trended for quality improvement purposes.		
Staff members are tested for knowledge and proficiency regarding software applications and computer connectivity.		
TMH-related policies, procedures and staff training efforts are reviewed on an annual basis, with revisions based upon incident report findings and assessment of the program's safety, effectiveness and efficiency.		
TECHNICAL ISSUES		
The organization has established technical specifications that promote safe and effective delivery of care, addressing such areas as:		
- Interoperability with partners.		
- Bandwidth.		
- Verification of data transmission.		
- Equipment maintenance.		
- On-site technical support.		
The selected technology model is user-friendly and provides seamless integration of patient/client data and services.		
Equipment is catalogued by make, model and serial number, and is tested for interoperability prior to use.		
Warranties are retained for all TMH equipment, and all equipment records are filed for easy reference.		
TMH equipment is physically secured in a locked area when not in use.		
A communication plan is established and implemented to inform staff swiftly of technical glitches – such as a disconnection with the remote site during a consultation – that may affect clinical outcomes.		
PRIVACY AND SECURITY PROVISIONS		
Appropriate security measures are implemented during the transmission process, including:		
- Authentication.		
- Patient/client identification.		
- Data control and tracking.		
- Wi-Fi protected access.		
Policies and procedures are established and implemented to protect the confidentiality of patient/client information, including:		
- Electronic privacy (e.g., use of passwords and encryption).		
- Physical site security.		
- Safeguarding the confidentiality of store-and-forward images and other patient/client records.		
- Agreements for all personnel involved in TMH, including vendor staff.		
TMH documentation formats are standardized and integrated with electronic patient/client health information records.		

RISK CONTROL MEASURES	STATUS	COMMENT/ ACTIONS PLAN
CONSULTATION ENVIRONMENT		
TMH sessions take place in a clinical setting that offers both privacy and professional amenities, analogous to traditional face-to-face consultations.		
The consulting space is well-lit, well-ventilated and well-equipped for safe patient/client examination, with an emergency alert system and easy access to infection control supplies.		
Consulting spaces are identified by signs, indicating that a private patient/client session is in progress.		
A comfortable waiting area is available for use by patients/clients and families.		
CLINICAL AND OPERATIONAL GUIDELINES		
Appropriate TMH clinical protocols are in use, which have been developed and reviewed by healthcare providers, and which address the full range of clinical events before, during and after consultation.		
TMH staff roles and responsibilities are incorporated into formal policies, which are reviewed and updated regularly.		
A formal process exists for obtaining informed consent of patients/clients for TMH services, encompassing full disclosure of known clinical and technical risks.		
Uniform referral and scheduling guidelines are drafted and included in partnership agreements.		
There is a formal policy for reserving TMH equipment and space, which includes a conflict resolution protocol.		
All TMH policies and procedures are reviewed comprehensively for compliance with extant regulations relating to patient/client safety and privacy.		
A consistent patient/client registration process is implemented for distant site facilities.		
The telepresenter has ready access to necessary communications equipment, including a computer, telephone and facsimile machine.		
Guidelines exist for telemedical testing, patient/client notification and follow-up procedures, with results documented in the patient/client health information record.		
Staff members acknowledge in writing their receipt of all relevant TMH policies and procedures, and are tested on their comprehension.		
CLINICAL AND OPERATIONAL GUIDELINES		
A standard method of collecting and storing TMH information is established and implemented at both originating and distant sites.		
A private and secure computer network is maintained to protect patient/client confidentiality and the integrity of information exchanged between sites/practitioners.		
Policy prohibits the use of personal e-mail accounts for the exchange of patient/client protected health information, instead mandating the use of network-based accounts.		
The TMH coordinator is swiftly notified of any changes regarding contact information of partner sites or practitioners, including business e-mail addresses.		

This tool provides a reference for organizations to evaluate risk exposures associated with the practice of telemedicine/telehealth. The content is not intended to be a complete listing of all actions needed to address the subject matter, but rather is a means of initiating internal discussion and self-examination. Your clinical procedures and risks may be different from those addressed herein, and you may wish to modify the tool to suit your individual practice and patient/client needs. The information contained herein is not intended to establish any standard of care, serve as professional advice or address the circumstances of any specific entity. The statements expressed do not reflect a risk management directive from CNA. No organization or individual should act upon this information without appropriate professional advice given after a thorough examination of the individual situation as well as relevant laws and regulations. CNA assumes no responsibility for the consequences of the use or nonuse of this information.

RESOURCES

The following additional sources offer a more detailed framework of guidelines, standards and tools for the safe practice of tele-medical diagnosis and care:

Publications

- California Telemedicine and eHealth Center, "Assessing Organizational Readiness" (January 2009).
- Center for Connected Health Policy, "State Telehealth Laws and Medicaid Program Policies" (March 2016).

Organizations

- American College of Radiology
- American Telemedicine Association
- Centers for Medicare and Medicaid Services
- The Joint Commission
- Office for the Advancement of Telehealth
- Telehealth Resources Center

866-262-0540 www.cna.com/healthcare

1-888-288-3534 www.nso.com www.hpso.com

Healthcare Perspective is a limited-edition publication for healthcare business owners. This series explores a range of relevant risk management concepts and offers strategies to detect and mitigate risks.

Published by CNA. For additional information, please contact CNA at 1-866-262-0540. The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situation. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. "CNA" is a service mark registered by CNA Financial Corporation with the United States Patent and Trademark Office. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities. Copyright © 2017 CNA. All rights reserved. Healthcare Providers Service Organization and Nurses Service Organization are registered trade names of Affinity Insurance Services, Inc. (AR 244489); in CA & MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services Inc.; in CA, Aon Affinity Insurance Services, Inc. (0G94493), Aon Direct Insurance Administrators and Berkely Insurance Agency; and in NY, AIS Affinity Insurance Agency. Published 6/17. Healthcare Perspective 14.