Healthcare

VANTAGE POINT®

A Risk Management Resource for Hospitals and Health Systems | 2021 Issue 2

Telemedicine: A Brief Guide to the Emerging Risks of Remote Care

The advent of the Internet has reshaped many areas of life, including the practice of medicine. As the virtual realm has grown, the traditional in-person encounter between healthcare provider and patient has become supplemented by telemedicine (TM), in which providers connect electronically with patients for such purposes as health screening, specialty consultation, and diagnosis and treatment of disease.

Telemedicine is one aspect of the broader practice of telehealth (TH), which encompasses a range of clinical services, including patient monitoring, counseling and education, as well as administrative functions delivered via patient portals, text messaging and email. The scope of telehealth capabilities has expanded dramatically in recent years due to a proliferation of technological innovations, including wearable and implantable devices, new software applications and interconnected health platforms. (See "Forms of Telehealth" on page 2.)

By 2017, **76 percent of U.S. hospitals engaged with patients through wireless communications and Internet-based systems**, compared with just 35 percent in 2010.

In this issue…

By 2017, 76 percent of U.S. hospitals engaged with patients through wireless communications and Internet-based systems, compared with just 35 percent in 2010. Already on an upward trajectory, virtual care has recently surged due to the COVID-19 pandemic and consequent restrictions on in-person clinical encounters. According to one source, providers reported seeing 50 to 175 times more patients via telehealth after the pandemic struck than before its onset. It is not yet clear if this remarkable expansion in remote care signals a permanent shift in healthcare delivery, as some caution in regard to TM/TH has been expressed recently at the federal level. (See sidebar, page 3.) However, considering the convenience and efficiency of TM/TH services, and the general trend toward connecting digitally with patients, these technologies will probably continue to flourish even after the pandemic wanes.

Forms of Telehealth

Telehealth – also known as *telemedicine, digital health, e-health* and *virtual care* – refers to healthcare services delivered remotely using advanced electronic technology. Some of the more common telehealth modalities are described below:

Form:	Definition:	Examples and uses:
Video conferencing	Live two-way interaction between patient and healthcare provider using audiovisual telecommunications technology.	• **Real-time healthcare services** and consultations for remote patients. • **Annual wellness visits** to clinics and medical offices. • **Collaborative consultation,** medical diagnosis and treatment by physicians and other providers based in different locations. • **Convenient referrals** to physically distant specialty providers. • **Emergency and critical care** in outlying locations, including prompt assessment of patients and consultation with specialists. • **Mental health services** for rural-based or underserved patients.
Store-and-forward or asynchronous video	Electronic transmission of patient health and medical data to a healthcare provider, who then treats the patient at a later time.	• **X-rays, MRIs, photos and other images** used for diagnostic purposes by primary or specialty providers. • **Prerecorded video clips** of patient examinations used to enhance the diagnostic process. • **Patient data** – including electronic health records, laboratory reports and medication management files – transmitted to specialists for use in consultations. • **Translated healthcare records** of non-English-speaking patients to facilitate provider treatment or consultation.
Monitoring and diagnostics	Electronic collection of patient data via "wearables" and "implantables," in order to enhance clinical monitoring and treatment of conditions.	• **Physiological data** – including blood pressure, heart rate, weight, and levels of oxygenation and blood sugar, among other metrics – gathered in real time. • **Comprehensive reports on chronic diseases** – e.g., diabetes, hypertension, asthma – used for data-driven decision-making and virtual patient education. • **Device-initiated alerts** to providers regarding patient noncompliance with diet recommendations, activity directives and other aspects of the treatment/care plan.
Mobile health or "mHealth"	A subset of telehealth that – using software applications designed for smartphones and other handheld communication devices – focuses on educating patients as well as connecting them electronically with their providers.	• **Personalized educational applications** that promote patient self-management of medical conditions, such as asthma and diabetes. • **Tools that integrate with electronic health records** and offer providers a more detailed view of a patient's medical history. • **Interfaces with wearable tech devices** that facilitate real-time review of patient data by members of the healthcare team. • **Automated reminders** to change surgical dressings, take medications or otherwise follow post-procedure recovery instructions.

GAO Raises Questions About Efficacy, Efficiency of TM/TH

In May 2021, the Government Accountability Office (GAO) testified to Congress that more research is needed before the decision is made to permanently expand telemedicine and telehealth (TM/TH) coverage for Medicare and Medicaid recipients.

Acknowledging that, for safety reasons, remote visits were essential during the pandemic, the GAO expressed uncertainty as to the effects of electronic encounters on quality of patient care. In addition, the GAO observed that greater utilization of TM/TH capabilities could increase program expenses, as some safeguards have been suspended during the COVID-19 emergency. Noted one GAO official, "Careful monitoring and oversight is warranted to prevent potential fraud, waste and abuse."

The GAO testimony was in response to bills introduced in both the House and Senate to retain certain TH-related flexibilities for Medicare and Medicaid beneficiaries – including elimination of originating site requirements – that were implemented when COVID-19 struck in the spring of 2020. In the absence of new legislation, these rule relaxations are scheduled to expire when the pandemic ends.

The debate at the federal level indicates just how rapidly virtual care is evolving. As the coronavirus crisis ebbs and flows, healthcare leaders need to reassess all aspects of TM/TH on an ongoing basis and remain alert to shifts in the legal, regulatory and payer environment.

Sources: King, R. "New House, Senate Bills Aim to Make Telehealth Expansion Permanent in Medicare, Medicaid." *Fierce Healthcare*, May 25, 2021. Mitchell, H. "GAO Tells Congress to Halt Expanding Telehealth Until There's More Research." *Becker's Hospital Review*, May 20, 2021.

As with **any major change** in medical practice, **potential ramifications of telemedicine** include an array of associated **liability exposures**.

As with any major change in medical practice, potential ramifications of telemedicine include an array of associated liability exposures. In an age of swiftly evolving and maturing TM/TH capabilities, all types of healthcare organizations should consider reviewing and enhancing their risk management programs with respect to remote care. This edition of *Vantage Point*® focuses on five key areas of concern:

- **Rapidly changing regulations** and related compliance issues.
- **Provider licensure laws** and ongoing reform efforts.
- **Delegation requirements and documentation standards for licensed, non-physician providers,** including physician assistants and advanced practice nurses, who deliver a significant amount of virtual care in some settings.
- **HIPAA exposures** connected to use of digital platforms.
- **Vendor assessment** and due diligence.

In addition, a checklist of documentation safeguards is included on pages 8-12 to aid providers and organizations in creating a clear and defensible record of virtual care and demonstrating compliance with regulatory parameters.

Maintain an agile, responsive regulatory compliance program. Legal obstacles restricting the use of TM/TH services have been relaxed during the pandemic, in order to enhance safety and increase patient access to healthcare providers and organizations straining to meet the unprecedented demand for their services. The Coronavirus Aid, Relief, and Economic Security (CARES) Act – which permitted delivery of remote services to a wider range of patients, regardless of their location and underlying condition – was enacted by Congress in March 2020. In addition, the Centers for Medicare and Medicaid Services (CMS) modified existing regulations to make it simpler for providers to offer virtual care services outside of previously designated rural areas, across state lines, and to both new and established patients.

Financial and technological factors also have contributed to the movement toward virtual care. Health insurers have increased reimbursement for remote services, while online platforms for virtual care have expanded to include Zoom, Skype and FaceTime, among other popular and user-friendly options.

The situation is fluid, and the easing of TM/TH-related regulations and other changes may not continue post-pandemic. (See sidebar at left.) As federal and state agencies begin to establish a longer-term legal framework, healthcare organizations should be on the alert for the issuance of further directives and updates relating to telemedicine. The following measures can help strengthen compliance during this time of rapid change:

Create a chronological inventory of regulatory changes. The compliance program's files should be well-organized, providing easy access to important dates, such as exactly when notice was received of new directives and when this information was conveyed to providers and staff. The filing system should also be user-friendly, permitting easy dissemination of directives to staff and providers via training forums, email, text messaging and institutional websites.

Digitally document compliance activities. In the event of a regulatory action, state and local surveyors will request a comprehensive record of compliance efforts. An electronic repository of telemedicine-related protocols, updates, communications and other actions can help strengthen defensibility against potential claims. The following compliance efforts, among others, should be documented:

- **Adoption or revision of policies and procedures** in response to legal/regulatory actions.
- **Training of providers and staff** on the scope and timeline of virtual care initiatives.
- **Administrative review of policies involving areas of high risk exposure,** including provider licensing and credentialing, patient privacy and confidentiality, and claim submission for virtual care services.

Is State-based Provider Licensing a Major Roadblock to Virtual Care?

The temporary easing of licensure requirements due to the pandemic has renewed the debate over interstate licensing of remote care providers. Some critics believe that our current state-based approach to licensing is obsolete and should be updated to enable wider use of telemedicine, thus increasing efficiency, convenience and patient access to care.

The discussion of regulatory alternatives continues. One proposal involves issuing a federal license to providers who practice telemedicine across state lines, in addition to their active state license. While the idea has garnered some degree of popular support, others view it as undermining the disciplinary function of state-based licensure systems.

For more information about licensing reform issues and efforts, see Svorny, S. "Liberating Telemedicine: Options to Eliminate the State Licensing Roadblock." Cato Institute, November 15, 2017.

Remain abreast of provider licensure requirements. After decades of discussion about the possibility of easing virtual care restrictions, TM/TH licensure laws and regulations remain primarily within the purview of individual states. At the height of the pandemic crisis, CMS temporarily waived the in-state licensure requirement for Medicare and Medicaid patients. Soon afterward, a number of states lifted similar restrictions in order to facilitate interstate practice. However, the vast majority of states continue to require that physicians and other providers who engage in virtual care be licensed in the state where the patient is located. (See sidebar at left.)

Given the legislative volatility regarding interstate licensure, it is imperative that hospitals and other healthcare organizations review current licensing requirements in their jurisdiction when verifying a provider's authorization to legally practice TM/TH. (For a state-by-state listing of licensure standards and policy statements, visit the Federation of State Medical Boards.) In addition, organizational leadership should remain cognizant of the following interstate reform measures designed to facilitate remote practice:

- **Interstate licensure compacts,** which build upon the current state-based medical licensing system by permitting providers to obtain an out-of-state license from participating state members.
- **License reciprocity,** under which certain states mutually honor one another's provider licenses. (Note that some states issued reciprocity declarations as a means of suspending in-state licensure requirements during the pandemic crisis.)
- **Telehealth-specific licenses,** whereby states grant temporary licensure to provide needed services remotely across state lines. These temporary provisions typically include certain restrictions for providers, such as agreeing not to open a physical office in the authorizing state.

Clarify the basic parameters of remote care delivery.

It is essential to delineate the parameters of virtual care delivery and to communicate these protocols to applicable practitioners. While the following suggestions generally apply to any providers authorized to deliver TM/TH care, they are particularly relevant to advanced practice providers, especially in terms of licensing, scope of practice, documentation and supervision:

Approved providers. Know what types of providers are permitted to engage in virtual care. Depending upon jurisdiction, authorized telehealth providers may include not only physicians, but also nurse practitioners, clinical nurse specialists, physician assistants, and licensed counselors and therapists. The following resources explore the issue of who is approved to provide TM/TH care:

- APRN Compact Legislation, a proposal that, if enacted, would institute a multistate license permitting advanced practice registered nurses (APRNs) to practice in all compact states.
- Association of Social Work Boards (ASWB), which provides current information on licensing and regulatory requirements and State Executive Emergency Orders.
- Garber, K. and Chike-Harris, K. "Nurse Practitioners and Virtual Care: A 50-State Review of APRN Telehealth Law and Policy." *Telehealth and Medicine Today*, June 2019.
- The Psychology Interjurisdictional Compact (PSYPACT), which authorizes eligible psychologists to practice telepsychology across member state lines.
- State Telehealth Laws and Reimbursement Policies, a report issued by the Center for Connected Health Policy, a program of the Public Health Institute, April 2021.
- Telehealth Licensing Requirements and Interstate Compacts, a compendium included on the U.S. Department of Health and Human Services telehealth website.

Licensing. Verify the provider's authority to deliver virtual care with the relevant governing body, such as the licensing board for nurse practitioners, social workers, or therapists and psychologists.

Scope of practice. Delineate prescribing parameters for advanced practice providers, as well as permitted TM/TH services and treatments, in conformity with state regulations, organizational policies, patient population needs, and available human and technical resources.

Follow-up. Prepare protocols addressing communication and follow-up requirements with supervising physicians, if relevant.

Telehealth training. Educate advanced practice providers and other authorized clinicians on the proper use of telehealth technology. If possible, schedule mock patient visits to ensure that practitioners are comfortable with TM/TH tools and procedures, and utilize practice modules focusing on how to properly respond to equipment and software glitches.

Patient selection. Not every patient is a suitable candidate for remote care. Adopt formal selection criteria, taking into consideration medical factors as well as Internet access and computer skills.

Patient verification. Confirm patient identity prior to TM/TH encounters, in order to prevent identity theft and fraudulent insurance billing.

Patient disclosure. Inform patients in writing when a nurse practitioner or other approved non-physician provider is delivering TM/TH services, including the signature of the practitioner and his or her licensing/certification designation.

Patient privacy. Remember that HIPAA requirements remain intact and are as applicable to TM/TH consultations as they are to in-person visits. Using two-way video interface platforms and other related communication applications, ensure that authorized providers receive adequate, documented training on how to securely share information with remote sites.

Documentation. Document virtual care delivery in the patient's healthcare information record in accordance with the organization's standards for in-person care. In general, virtual care notations should include patient history, review of systems, information used to make treatment decisions, follow-up instructions, referrals to specialists and discussions with supervising physicians, if necessary. All patient-related electronic communications should be included in the patient healthcare information record. In addition, note that the service was provided through interactive telecommunications technology, indicating the location of the patient and the provider, as well as the names and roles of other persons participating in the virtual event.

Audit TM/TH care. Following remotely held sessions, share care-related information – including adverse events and any complaints received about any of the providers – between the originating and distant site.

Address potential HIPAA exposures associated with digital communication platforms.

At one time, FaceTime, Zoom, Skype and other consumer-based video communication platforms were not extensively used in the healthcare context due to security and privacy concerns, especially regarding their data encryption limitations and the potential for third-party eavesdropping. Recently, however, the U.S. Department of Health and Human Services has authorized their use – as well as messaging applications such as WhatsApp and Viber – in order to facilitate provider-patient contact during the pandemic. The agency is also exercising discretion pertaining to enforcement of HIPAA privacy laws, stating that providers who utilize these digital tools in good faith will not be penalized for noncompliance.

Tips for Video Conferencing from the Homes of Providers

1. **Update the organization's virtual private network (VPN)** with software patches and security configurations, in order to ensure safe transmission of data from providers' home networks through the VPN.
2. **Monitor and test the limits of the VPN** in anticipation of increased network traffic, and make adjustments for providers who require increased bandwidth.
3. **Require that users provide authentication before logging onto the VPN,** and educate providers about the risk of "phishing" attempts – i.e., fraudulent efforts to persuade users to reveal personal information for purposes of identity theft – by computer hackers.
4. **Guard against computer viruses and other malware** by installing effective security software on all devices connected to the VPN.
5. **Ask providers to designate themselves as sole system administrator on their personal home network** and to change their network router password frequently.
6. **Direct providers to select a new password for each video conference** and refrain from disclosing private information about the conference subject in meeting notices.
7. **Advise providers to store all patient care data on a secure laptop or other device** that is separate from their main home computer system.
8. **Strictly prohibit sharing of sensitive files during virtual meetings,** instead utilizing secure file-sharing technologies for this task.

The extent to which hospitals and other healthcare organizations will continue to employ these technologies once the federal enforcement discretion is lifted remains unclear. Their continued usage may depend upon the platforms' ability to safeguard data and protect patient confidentiality. The following actions, among others, can significantly enhance privacy during video conferencing and minimize the potential for security breaches:

- **Implement technical safeguards to protect electronic health information,** including password-protected access to software applications, end-to-end encrypted data transmission, formal procedures for obtaining patient information during emergency consultations and automatic log-off times.
- **Draft a medical staff protocol** to ensure that only trusted, authorized providers are granted privileges to engage with patients through video conferencing technologies.
- **Verify that telecommunication platforms can interface with desktop computers and audiovisual equipment,** as well as connect with tablets, smartphones and other handheld devices.
- **Select products offering encrypted chat features,** so that multiple parties can safely participate in conferences.
- **Ensure that video conference hosts can maintain full control of meetings** by limiting participation and expelling unauthorized attendees.
- **Create effective privacy features for conferencing,** including password-protected access to chat rooms, passcodes for digital waiting rooms and locked room protections.
- **Routinely test privacy control features,** such as mute/unmute settings for participants and locks that restrict screen sharing.
- **Establish a security protocol for providers who work from home, Internet cafes or other remote locations,** and ensure that the protocol is aligned with HIPAA privacy requirements. (See "Tips for Video Conferencing from the Homes of Providers," at left.)

Healthcare organizations that currently use consumer video conferencing applications are encouraged to migrate to a healthcare-specific, HIPAA-compliant platform designed to accommodate their unique needs. In addition, organizations may need to enhance their technical and administrative cybersecurity infrastructure to help combat security threats associated with increased online traffic.

Conduct due diligence regarding vendors.

There are many vendors of TM/TH products and services, and selecting the safest and most suitable tools requires careful consideration of multiple factors, including system capabilities, technical specifications, compatibility with existing digital infrastructure, privacy features and post-sale service.

After performing preliminary product and vendor research, submit a formal Request for Information (RFI). RFIs should request a range of information from vendors, including the following:

- **The vendor's profile** (e.g., ownership arrangement, size of workforce, domicile, years in business).
- **Total money allocated to research and development,** a sign of commitment to quality and innovation.
- **Proof of product compliance with HIPAA requirements,** such as HITRUST Alliance certification or a similar vetting.
- **Presence of certified trainers** specializing in healthcare applications.
- **Names of comparable healthcare clients** who can provide references.
- **Extent of the product's mobile compatibility,** permitting providers to access information through their smartphones or other handheld devices.
- **Availability of on-site and web-based training,** as well as 24/7 customer support.
- **Software licensing arrangements** and associated user fees.
- **Means of documenting patient interactions** when using the product or service.
- **Implementation costs,** including hardware and software requirements, staff training, program maintenance and upgrades, and patient education on use of web-based portals.

When acquiring digital applications from a vendor, a user license is generally considered preferable to a subscription arrangement. By purchasing a software license, organizations obtain ownership of the product and exercise full control of the data. By contrast, a subscription often involves centralized data storage by the vendor, which could potentially lead to third-party interference. In either case, request that vendors sign a Business Associate Agreement to ensure they remain legally accountable for HIPAA privacy and security regulations. Consult with legal counsel regarding contractual arrangements with vendors and applicable conditions and provisions.

For a variety of reasons – including evolving technology, mounting economic pressures and the lingering impact of the COVID-19 pandemic – telemedicine/telehealth utilization has expanded considerably in recent years. While promising increased patient access and safety, virtual care also presents significant liability and compliance exposures. By remaining cognizant of changing regulations, and implementing sound protocols in such basic areas as provider licensure and training, verification of patient identity, service documentation and vendor selection, healthcare organizations can minimize the risks associated with remote care while maximizing the efficiency and convenience of this innovative healthcare delivery mode.

Quick Links

- "Clinician's Guide to Video Platforms," from the National Telehealth Technology Assessment Resource Center.
- National Consortium of Telehealth Resource Centers.
- "Practical Guidelines for Video-based Online Mental Health Services," from the American Telemedicine Association.
- "Practice Guidelines for Telehealth," from the American Telemedicine Association.
- Resources from the National Telehealth Technology Assessment Resource Center.
- "Telehealth: Health Care From the Safety of Our Homes," from the U.S. Health and Human Services Department, Health Resources & Services Administration.
- "Telehealth Quick Guide," from the American Medical Association.
- "Telemedicine: Connect to Specialists and Facilitate Better Access to Care for Your Patients," from the American Medical Association.

Checklist: Creating a Defensible and Compliant Record of Virtual Care

Compliance Measures	Status	Action Plan
Basic Business and Operational Considerations		
A written protocol is created, which delineates acceptable uses of remote care technologies, e.g., prescription refills, appointment scheduling, assessment, patient and specialist consultation, and education, among others.		
A thorough, documented due diligence evaluation is conducted of potential telemedicine and telehealth (TM/TH) partners, especially with regard to clinical and technical compatibilities.		
A business associate agreement is signed with all TM/TH partners, pursuant to HIPAA privacy rule requirements.		
A record is maintained of TM/TH partners' contact information, including business email addresses.		
A "memorandum of agreement" is written, reviewed by legal counsel and entered into with partner sites.		
The memorandum is checked to ensure that it provides specific answers to key questions about the partnership arrangement, including the following:		
• Who provides support staff?		
• Who pays for telecommunication connections?		
• Who supplies and maintains equipment?		
• What space is available for TM/TH encounters?		
• Who manages the billing process?		
A TM/TH coordinator is designated and a job description written, assigning the coordinator responsibility for providing administrative support for consultations/referrals, program functioning and system processes.		
A written TM/TH procedure manual is developed, which addresses a broad range of clinical processes that occur before, during and after consultations.		
The procedure manual is reviewed by affiliated healthcare providers to ensure that it conforms with practice guidelines issued by national associations.		
Uniform referral and scheduling guidelines are drafted and included in partnership agreements.		
A formal policy for reserving TM/TH equipment and space is promulgated, which includes a conflict resolution protocol.		
A written protocol is instituted to guide the patient selection process, which includes specific parameters for referral to TM/TH providers, such as patients who require the following types of treatment:		
• Chronic care management.		
• Acute, uncomplicated care.		
• Medication management.		
• Pre- and post-operative care.		
• Mental health therapy.		
• Nutrition services.		
• Specialty care referral.		

Compliance Measures	Status	Action Plan
Basic Business and Operational Considerations (continued)		
A consistent patient registration process is implemented for distant site facilities.		
Formal procedures are established for patient testing and notification, including documentation of test results and follow-up measures in the patient healthcare information record.		
A procedure to escalate care in emergency situations is adopted, which includes consulting with other providers, accessing backup technology for immediate use and arranging prompt in-person intervention if necessary.		
Provider Fitness and Preparedness		
Licensure verification records are maintained for physicians, nurse practitioners, physician assistants and other designated healthcare professionals (hereafter "providers") involved in the delivery of virtual care.		
TM/TH credentialing, privileging and peer review processes are developed for providers, reflecting patient safety, jurisdictional and liability considerations.		
Roles and responsibilities related to the provision of virtual care are clearly defined by regularly updated formal policies, which are disseminated to different medical disciplines and staff levels.		
Guidelines are adopted to ensure that TM/TH services are offered only when there is a professional relationship between the provider and the patient, as defined by the following criteria, among others:		
• **Knowledge of the patient and the patient's health status** through an ongoing personal or professional relationship.		
• **A previously conducted in-person examination** of the patient.		
• **Availability for appropriate follow-up care** at medically necessary intervals.		
• **Past treatment of the patient in consultation with another professional** who has an ongoing relationship with the patient.		
• **An on-call or cross-coverage arrangement** with the patient's regular treating healthcare professional.		
Providers are formally instructed and regularly informed that the same standard of care applies to both TM/TH services and in-person care, and it is neither modified, enhanced nor reduced simply because a patient visit is conducted remotely.		
Receipt of TM/TH-related policies and procedures is acknowledged in writing by providers, who are tested on their comprehension, including how and when to do the following:		
• Schedule a consultation.		
• Arrange for a consulting room.		
• Set up necessary equipment.		
• Establish network connections.		
• Prepare and advise the patient and consulting provider, if applicable.		
• Document consultation findings.		
• Secure and back up required data.		
• Prepare reports of virtual care episodes.		

Compliance Measures	Status	Action Plan
Provider Fitness and Preparedness (continued)		
Educational and professional development requirements are specified in writing, including participation in pilot programs, as well as familiarity with clinical protocols, equipment capabilities and documentation requirements.		
Providers and staff members are tested for general computer proficiency, as well as knowledge of software applications and device features and connectivity, and records are maintained of testing results.		
Providers are trained on an ongoing basis in virtual care protocols, including proper documentation practices.		
Staff members are trained in incident reporting, and adverse TM/TH occurrences are tracked and trended for quality improvement purposes.		
Technical Safeguards		
Organizational standards and technical specifications are developed to promote safe and effective delivery of care, covering such areas as bandwidth, interoperability, verification of data transmission, equipment maintenance and on-site technical support.		
A private and secure computer network is maintained to protect patient confidentiality and the integrity of data exchanged between sites and providers.		
Equipment and software are catalogued by make, model and serial number, and are tested for functionality and interoperability prior to use.		
Warranties on all TM/TH equipment are filed for easy reference, as are all equipment maintenance records.		
A system is created to swiftly inform staff of technical glitches – such as a disconnection with a remote site during a consultation – that may affect clinical outcomes.		
Privacy and Security Provisions		
All TM/TH policies and procedures are reviewed periodically for compliance with extant regulations relating to patient privacy.		
Rules are established regarding the virtual consultation process and environment, including the following, among others:		
• **TM/TH sessions are scheduled in a suitable clinical setting** that offers both seclusion and professional amenities, when possible.		
• **Consulting spaces are identified by clearly visible signs,** indicating that a private patient session is in progress.		
• **Appropriate security measures are implemented during the transmission process,** including such critical functions as authentication, patient identification, data control and tracking, and Wi-Fi protected access.		
Measures are taken to protect the confidentiality of patient information, including the following, among others:		
• Electronic privacy safeguards, such as use of passwords and/or encryption.		
• Physical site security.		
• Securing of store-and-forward images and other patient records.		
• Confidentiality agreements for all personnel involved in TM/TH, including vendor staff.		

Compliance Measures	Status	Action Plan
Privacy and Security Provisions (continued)		
Providers are trained to comply with HIPAA, CMS, CDC and other state and federal regulations and guidelines relating to protection of patient privacy and confidentiality.		
A policy is adopted prohibiting use of personal email accounts for the exchange of protected patient health information, and mandating use of network-based accounts or secure, facility-approved messaging applications.		
Clinical Documentation and Recordkeeping		
A standard method of collecting and storing TM/TH information is implemented at both originating and distant sites, if applicable.		
TM/TH documentation formats are standardized and integrated with electronic patient health information records.		
Virtual care encounters are thoroughly documented, including, but not limited to, the following information:		
• Patient name and identification number.		
• Originating facility's name.		
• Distant facility's name, if applicable.		
• Registration information (i.e., patient identification number and provider assignment) at distant site, if applicable.		
• Date of service.		
• Referring provider's name, if applicable.		
• TM/TH provider's name.		
• Type of evaluation to be performed.		
• Informed consent form and signature.		
• Diagnosis/impression of providers.		
• Recommendations for further treatment.		
A formal process is established for obtaining and documenting patients' informed consent for TM/TH services, encompassing the following information, per the Federation of State Medical Boards:		
• Patient identification, including name and date of birth.		
• Names, credentials, organizational affiliations and locations of physician and/or other healthcare professionals involved in the visit.		
• Name and description of the recommended procedure.		
• Potential benefits and risks of the procedure.		
• Possible alternatives, including no treatment.		
• Risks of declining the treatment/service.		
• Confirmation that patient understands and accepts remote care delivery mode.		
• Contingency plans in the event of technical problems during the procedure.		
• Explanation of how care is to be documented and accessed.		
• Security, privacy and confidentiality measures to be employed, as well as extent of risk to privacy notwithstanding such safeguards.		
• Names of those responsible for ongoing care.		
• Reiteration of the right to revoke consent or refuse treatment at any time.		
• Consent of patient to forward patient-identifiable data to a third party.		

Compliance Measures	Status	Action Plan
Quality Improvement		
A formal TM/TH quality improvement program and review process is implemented, which tracks the following quality of care indicators, among others:		
• Equipment or connectivity failures.		
• Number of attempted and completed visits.		
• Average waiting times.		
• Patient and provider satisfaction with virtual patient encounters.		
• Patient or provider complaints related to virtual visits.		
Outcome metrics are decided upon to monitor and assess the clinical quality and efficiency of virtual care encounters, including the following:		
• Patient complication and morbidity rates.		
• Provider compliance with performance criteria, including productivity and patient satisfaction levels.		
• Diagnostic accuracy.		
• Adherence to evidence-based clinical protocols.		
• Referral rates.		
• Cost per case.		
• Delays in accessing consultations, referrals or specialty practitioners.		
Outcome findings are reported to the Quality Improvement Committee (QIC) on an ongoing basis.		
Written guidelines are developed for auditing TM/TH practitioners and sharing internal review information – including virtual care-related adverse events – with established quality improvement and risk management programs.		
TM/TH-related policies, procedures and staff training efforts are reviewed every six to 12 months, with revisions based upon incident report findings and assessment of the program's overall safety, effectiveness and efficiency.		
Regular equipment testing and maintenance is performed and documented, including post-installation testing and pre-session calibration, as well as ongoing quality checks of audio, video and data transmission capabilities.		
Routine audits of equipment and software functionality are conducted, and reports are prepared for the QIC.		

This resource serves as a reference for healthcare organizations seeking to evaluate risk exposures associated with telemedicine and telehealth. The content is not intended to represent a comprehensive listing of all actions needed to address the subject matter, but rather is a means of initiating internal discussion and self-examination. Your organization and risks may be different from those addressed herein, and you may wish to modify the activities and questions noted herein to suit your individual organizational practice and patient needs. The information contained herein is not intended to establish any standard of care, or address the circumstances of any specific healthcare organization. It is not intended to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. The material presented is not intended to constitute a binding contract. These statements do not constitute a risk management directive from CNA. No organization or individual should act upon this information without appropriate professional advice, including advice of legal counsel, given after a thorough examination of the individual situation, encompassing a review of relevant facts, laws and regulations. CNA assumes no responsibility for the consequences of the use or nonuse of this information.

Editorial Board Members
Kelly J. Taylor, RN, JD, *Chair*
Janna Bennett, CPHRM
Peter S. Bressoud, CPCU, RPLU, ARe
Lauran L. Cutler, RN, BSN, CPHRM
Hilary Lewis, JD, LLM
Lauren Motamedinia, J.D.
Katie Roberts

Publisher
Patricia Harmon, RN, MM, CPHRM

Editor
Hugh Iglarsh, MA

Did someone forward this newsletter to you? If you would like to receive future issues of *Vantage Point*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

CNA Risk Control Services: Ongoing Support for Your Risk Management Program

CNA provides a broad array of resources to help hospitals and other healthcare organizations remain current on the latest risk management insights and trends. Bulletins, worksheets and archived webinars, as well as past issues of this newsletter, are available at www.cna.com/riskcontrol.

Your SORCE® for Education

CNA's School of Risk Control Excellence (SORCE®) offers complimentary educational programs that feature industry-leading loss prevention and risk transfer techniques. Classes are led by experienced CNA Risk Control consultants.

SORCE® *On Demand* offers instant access to our library of risk control courses whenever the need arises. These online courses utilize proven adult-learning principles, providing an interactive educational experience that addresses current regulatory requirements and liability exposures.

Allied Vendor Program

CNA has identified companies offering services that may strengthen a hospital's or other healthcare organization's risk control program and help it effectively manage the unexpected. Our allied vendors assist our policyholders in developing critical programs and procedures that will help create a safer, more quality-focused environment.

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare.

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 © 2021 CNA. All rights reserved. Published 7/21. CNA VP21-2.