CNA NSO HPSO

Risk Management Strategies for the Outpatient Setting

Risk Management Strategies for the Outpatient Setting

Technology and Electronic Media

Contents

Electronic Documentation

Electronic media – including email, blogs, social networking platforms, websites, texting and instant messaging have become a primary means of self-expression and communication for many individuals, including providers and other medical practice personnel. The increasing volume of online communications and instant messaging has created a new sense of connectedness – as well as a myriad of risks, including electronic discovery requests that may encompass text messages, blog entries and social media postings.

The substance of all electronic communications related to patient care – whether by phone, text, email or instant messaging should be documented in the patient's healthcare information record.

At a minimum, the following information should be included when documenting any electronic communication:

- Date and time of the discussion
- Patient's name and date of birth
- Identity of the other party (if other than the patient)
- Identity of the staff member involved in the communication
- Subject of the communication
- Advice given or other outcome and recommended follow-up

The following clinical information also should be included, among others:

- Patient's relevant medical history and allergies
- Nature of the patient's symptoms and associated complaints
- Aggravating and relieving factors

Electronic Media Exposures

The risks associated with electronic media continue to evolve and expand with increased usage. Providers should be aware that litigation discovery requests may transcend the traditional scope of patient treatment and financial records, potentially encompassing text messages, blog entries and social media postings. Consequently, providers must understand the associated exposures and create policies that recognize their benefits while minimizing the possibility of carelessness or misuse. The use of social media and electronic devices by healthcare personnel may result in the following additional risk exposures, among others:

Patient confidentiality. Workplace emailing or text messaging may violate privacy and security requirements imposed under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), as protected health information (PHI) may be inadvertently transmitted to an unauthorized third party. If protected health information (PHI) is inadvertently revealed on organization-owned equipment or employee-owned devices, disclosure may constitute a breach of the HIPAA Privacy Rule and the Security Rule, as well as related state laws. The use of cellular telephones and smartphones to take and share photographs relating to a patient has significant privacy implications. Every healthcare setting should consider implementing a HIPAA compliance program that encompasses ongoing staff training, review of protocols and technical upgrades, including use of a HIPAA-compliant encrypted email system. A wide range of resources and tools are available to aid medical practices in this effort , including resources from the US Department of Health and Human Services and CMS.

Improper texting. Harassing, threatening or otherwise inappropriate messages posted by employees from workplace computers, texted from employer-issued mobile telephones, or employee-owned equipment can create vicarious liability exposures for the healthcare practice. In addition, improper litigation-related postings and text messages can undermine legal defense efforts.

Overuse of electronic devices. Texting and conversing on cellular telephones in patient care areas may decrease staff efficiency, leading to distraction and patient safety issues.

Network security issues. Unregulated web browsing and emailing on networked computers can introduce viruses or spyware into the system, resulting in possible data loss, theft or damage. Sharing of passwords and other security lapses can compromise confidential information, with potentially serious regulatory and liability implications.

Reputational risk from patient comments. Patients' use of electronic media, especially through blogs and online rating sites, creates reputational risk exposures for providers and practices. Many states have enacted laws that affirm the patient's legal right to offer a public opinion, even if that opinion is considered inaccurate or offensive to the provider. In general, legal cases in which providers challenge patient statements have not resulted in favorable outcomes for the providers.

Patient recruitment risks. Utilizing electronic media forums to recruit new patients or build loyalty may damage the reputation of a healthcare practice, unless the effort is managed in accordance with ethical guidelines. Risk exposures include, but are not limited to, jurisdictional issues and allegations of fraud and defamation.

Risk Management Strategies

Policies should directly address the issues raised by the proliferation of electronic media, in order to clarify rules and expectations and reduce liability exposure. These policies should clearly state that they apply to administrative, support and professional staff, as well as any contractors working for the organization.

The following strategies can help providers effectively manage the widespread use of these communication tools:

- **Create and enforce a formal policy governing personal use of networked computers,** with provisions that strictly prohibit all messages and activities of an offensive, threatening, harassing, defamatory or unprofessional nature.
- **Request that employees sign a form acknowledging that they understand the rules and the consequences of noncompliance.** Signed forms should be retained in personnel files.
- **Provide staff with written copies of electronic monitoring policies.** Explain that employers have the right to monitor email messages and other communications on practice-owned computers and that inappropriate conduct may have disciplinary consequences, up to and including termination.
- **Regulate cellular telephone use by staff members,** specifically addressing such key issues as personal telephone calls while at work, confidentiality, conversational volume and etiquette, talking while driving and utilization of the camera feature.
- **Revisit the privacy and confidentiality policies on a routine basis,** taking into consideration the risks of posted and texted messages containing PHI or other sensitive material.
- **Convey to staff the possible legal and ethical implications of the unprofessional use of email, texts and social media,** including the permanence and recoverability of deleted messages, limits of anonymity and realities of e-discovery. Clearly describe both the nature of the risks and the consequences of policy violations in the employee handbook, and reinforce the importance of sound judgment through staff training.
- **In consultation with administration and/or legal counsel,** formulate a protocol requiring written authorization from patients before discussing PHI on any electronic media or outside the patient care setting.
- **Encourage appropriate etiquette and model a mature attitude.** Remind staff members that they are viewed as ambassadors of the practice, and their posture on the internet should reflect this fact. Consider assigning mentors to coach less experienced staff in the nuances of professional conduct.
- **Regularly underscore cyber security rules and concerns,** using orientation and training sessions, posters, supervisory reminders and other means.
- **Have both legal counsel and information technology staff review all social media-related policies** for regulatory compliance and technical relevance.
- **Draft policies addressing the following important activities:** engaging e-patients, managing online discussions, conveying medical advice and general medical information, integrating electronic communications with the personal healthcare information record, and disengaging e-patients who publish derogatory statements or falsehoods about the practice.
- **Review marketing language used online to avoid inaccurate statements of services provided, avoiding use of** superlative and absolute phrases such as "best care," "highest quality" or "state of the art," as these descriptions may be quoted in lawsuits alleging breach of an express or implied warranty. In addition, social media messaging should not entice patients to expect care beyond the capabilities of the practice.
- **Adopt a HIPAA-compliant email encryption system** in order to better protect the confidentiality of sensitive information.

Social Media

Many healthcare organizations use social media for purposes of outreach, reputation management and emergency communication. They expand their networking ability by linking their practice-based websites to the following types of media platforms:

- **Social networking sites,** such as Facebook and Instagram, which promote mutual sharing of news and information, as well as marketing messages.
- **Video and photo-sharing sites,** including YouTube, Flickr, DropBox, Google Drive and OneDrive, which facilitate exchange of footage and images.
- **Micro-blogging sites,** such as Twitter, which encourage interaction via short published messages and links.
- **Weblogs,** including practice, personal and media blogs, which communicate ideas and opinions in journal format.
- **Business networks,** such as LinkedIn, which connect job seekers and potential partners to the practice or organization, and colleagues with each other.

Launching an effective social media site requires preparation, planning and attention to a number of risk management considerations. Before initiating a social media project, consider its implications from a strategic, marketing, liability and information security perspective. The following questions may help focus the planning process:

- **What is the underlying purpose** of the social media activity?
- **Does the proposed social media presence complement the business strategy?**
- **Who is the intended audience** for the site, page or profile?
- **Which topics, activities and forms of interaction will be promoted,** and which will be excluded?
- **Are adequate human and financial resources available** to maintain and update the project on an ongoing basis?
- **Which media platform, tool or application is best suited** to the intended purpose and audience?

Organizations may wish to retain a social media specialist to address these initial questions, as well as to assist in the planning and implementation of the following essential activities:

- **Establishing practical boundaries and guidelines** for electronic media use.
- **Promulgating sound operating rules and security controls** to protect against infiltration and other external threats.
- **Negotiating with vendor platforms regarding terms of use,** such as requirements for separate login pages and written notice of changes in privacy conditions.
- **Reviewing insurance policies** for potential cyber liability insurance coverage gaps and recommending portfolio changes, where necessary.

Once the site goes online, the social media consultant also can help to educate staff, patients and other users on rules and etiquette, advise on updating guidelines, assist legal counsel in reviewing and updating vendor contracts and site controls, and ensure that all social media tools have a consistent identity and appearance – including appropriate use and placement of the organization's logo.

Social Media Policies and Safety Measures

The many potential benefits of social media platforms for healthcare organizations are accompanied by an equally broad range of risk management considerations, which must be addressed by office policy. The following guidelines can help organizations retain control of this powerful tool and simultaneously minimize liability and regulatory exposure:

Incorporate social media issues into staff training. Sessions should include such key concerns as social networking protocol and expectations, parameters for use during working and non-working hours, potential legal ramifications, patient confidentiality issues and disciplinary consequences of misuse. Offer training to all employees and providers upon hire and annually thereafter, documenting session content and attendance.

Establish standard terms of use. Inform users that they are subject to the site's terms and conditions and that repeat violations will result in termination of access. The "click agreement" with users should be written in clear and unambiguous language and include these basic provisions, among others:

- **Users understand the risks associated with participating in online communication** and acknowledge that postings by providers and staff are not intended to be interpreted as a medical diagnosis or treatment.
- **Service marks and trademarks of the practice are the sole property of the organization,** and no copyrighted text, image, video or audio content may be distributed, modified, reproduced or used, in whole or in part, without prior written consent of the organization's leadership.
- **Blog postings may be edited or deleted by leadership without prior notice,** and abusive, illegal, disruptive or medically misleading communications are subject to immediate removal.
- **Disclosure of patient health information shall be governed by patient privacy policies,** as well as relevant federal and state privacy laws and regulations. Solicitation of confidential or proprietary patient information is strictly prohibited.
- **The practice is indemnified against any damages, liabilities, judgments or expenses** arising from any third-party claim involving posted material.

Prepare disclaimer statements. Sites should include the following standard disclaimers:

- **All content and information are of an unofficial nature** and are not intended to be interpreted as medical advice.
- **The views expressed are those of users** and do not necessarily represent those of the organization.
- **The sponsoring practice is not obligated to monitor chat rooms, Facebook pages, bulletin boards or other interactive areas** where visitors post their comments.

Institute strict editorial controls. Written guidelines for user-posted comments should include the following restrictions:

- **Postings cannot include specific patient data** or other confidential information.
- **No unlawful material can be posted on the site,** nor any content that could be considered obscene, defamatory, threatening, harassing or malicious.
- **No material can infringe on the rights of any third party,** including rights to intellectual property, privacy and branding.
- **Any off-topic material may be deleted,** including the promotion of outside products, services, groups or organizations.
- **The organization reserves the right to remove posts advertising commercial products,** including business solicitations, chain letters or pyramid schemes. Platform settings should disable advertisements and "pop-ups," where possible.
- **Users may not impersonate another individual** or share their identity and password.
- **Develop an incident response plan.** The written response plan should address violations of site rules, such as sharing of passwords, hacking, or posting of unauthorized patient images or other inappropriate content. At a minimum, the plan should encompass removal of objectionable material, notification of offenders, documentation and reporting of incidents, staff follow-up action and disciplinary standards, drafted in compliance with relevant employment laws and regulations.

Telehealth

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 the patient has become supplemented by telehealth. Telehealth (TH) refers to a broad range of remote patient care services, including clinical and non-clinical services. Videoconferencing, transmission of still images, patient portals, remote monitoring of vital signs, continuing medical education, and nursing call centers may be within the scope of telehealth.

Telemedicine (TM) is one aspect of telehealth. Telemedicine refers to delivery of clinical services provided at a distance through telecommunications in real-time. Through audio and visual technology, providers connect with patients using TM for healthcare services such as health screening, patient monitoring, counseling and education, specialty consultation, and diagnosis and treatment of disease.

Digital Health is another aspect of telehealth. Digital health includes health technology, digital tools, software and sensors to connect people and populations to manage health and wellness. Mobile health apps, electronic healthcare records, wearable devices are examples of digital health.

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.

Telemedicine (TM)

Implementation of TM as an accepted tool across the continuum of healthcare remains fluid as technology, licensing issues, costs, reimbursement, access, cybersecurity, and quality issues continue to evolve.

All providers using TM are held to the same professional practice standards as a provider practicing in the same profession or specialty, in an in-person setting. Consideration to the time of day, location, type of setting, and other variables will affect practice standards. Referral to a higher level of care is the responsibility of the provider.

Licensure and State Laws

TM licensure laws and regulations remain primarily within the purview of the individual states. The types of providers permitted to engage in telemedicine depends upon the jurisdiction. Requirements may include physicians, nurse practitioners, physician assistants, and some other licensed providers. Knowing the providers who are permitted to practice virtual care is the responsibility of the provider and facility.

Most states continue to require that providers who engage in telemedicine be licensed in the state where the patient is located. Federal and state waivers issued during a national healthcare emergency, such as a pandemic, expire and the regulations return to "pre-emergency" status. In view of the legislative volatility regarding interstate licensure, review current licensing requirements when verifying a provider's authorization to practice TM. State-by-state listing of licensure standards and policy statements are located at the Federation of State Medical Boards.

Telemedicine Training

Provider training is critical to successful implementation of TM. Training on TM can take the form of mock patient visits and practice modules designed by the software distributor. Training should be updated as new functions and upgrades are implemented.

At a minimum, training should seek to establish competency in video communication skills, documentation, understanding the scope and limitations of services provided via TM, proficiency with technology to be used and ability to troubleshoot unexpected equipment malfunctions.

Document all staff and provider training for TM. Permit only authorized providers, who have completed the required training and demonstrated an understanding of the unique issues, to provide healthcare via TM.

Establishing Provider-Patient Relationship

A patient-provider relationship can be established without a prior in-person visit or examination. Establishing a provider-patient relationship depends upon the following:

- Obtaining the patient's consent for the use of TM as the tool in which care will be delivered, and
- Verification of the patient's identity and disclosure of the provider's identity and credentials.

Document both of these steps in the patient's healthcare information record.

Standard of Care

Patient Selection – Not every patient is a suitable candidate for remote care. Formal selection criteria should be established that considers medical factors, as well as internet access and computer skills.

Consent – Obtain a verbal consent from the patient to proceed with providing healthcare via TM and document in the patient healthcare information record.

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

Documentation – All care delivered via TM must be documented in the patient's healthcare information record in accordance with the standards of documentation for in-person care. Such documentation includes patient history, review of systems, information used to make treatment decision(s), follow-up, referrals, any instructions given, and, where required, discussion with the supervising physician.

In addition, documentation should reflect that the service was provided through interactive TM technology, indicating the location of the patient and the provider, as well as the names and roles of other individuals participating in the virtual event.

Follow-up – Providers must impart patients with the means to contact the treating provider, or covering provider, for follow-up care and questions.

Prescribing medications – Providers must comply with all state and federal regulations for prescribing in the state where the patient is located and the provider is licensed to practice.

Safeguards

Privacy – All HIPAA requirements that apply to in-person encounters also apply to TM encounters. The use of healthcare specific, HIPAA compliant platforms is recommended.

Equipment and maintenance – Equipment should be suitable for diagnostic and treatment purposes, readily available when needed and fully functional during clinical encounters. Organizations should identify an individual with sufficient technical knowledge to be responsible for the maintenance and routine testing of equipment and privacy functions. User and administrator passwords should be changed every 90 days, at a minimum.

Cybersecurity – Install effective security software. 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 consultations and automatic log-off times.

Video conferencing from outside the secure office network – Two-way audio/visual interface platforms used outside a secure office network create additional privacy issues of which providers must be aware. When selecting and approving TM platforms for use, due diligence in evaluating the strength of the privacy and encryption capabilities is required. Install a virtual private network (VPN) with software patches and security configurations to ensure safe transmission of data and communications. Conduct periodic testing to ensure adequate bandwidth.

Selecting a TM Vendor

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 elements and post-sale service.

When conducting due diligence in selecting a TM vendor, consider the following:

- The vendor's profile (e.g., ownership arrangement, size of workforce, domicile, years in business).
- Total funds 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 onsite 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 considered preferable to a subscription arrangement. By purchasing a software license, organizations obtain ownership of the product and exercise full control of the data. In contrast, a subscription often involves centralized data storage by the vendor, which may potentially lead to third-party interference. In either case, request that vendors sign a Business Associate Agreement to ensure that they remain legally responsible for HIPAA privacy and security regulations. Consult with legal counsel regarding contractual arrangements with vendors and applicable conditions and provisions.

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.		

For more information, please call us at 215-509-5437 or visit www.nso.com or www.hpso.com.

Published 8/2023.

215-509-5437 www.nso.com www.hpso.com