CNA nso®

Nurse Practitioner Spotlight: Telemedicine

Nurses Service Organization (NSO), in collaboration with CNA, has published our 5th Edition of the NSO/CNA *Nurse Practitioner Liability Exposure Claim Report*. It includes statistical data and case scenarios from CNA claim files, as well as risk management recommendations designed to help nurse practitioners (NPs) reduce their malpractice exposures and improve patient safety.

You may access the complete report, and additional Risk Control Spotlights, at: www.nso.com/NPclaimreport.

This Nurse Practitioner Spotlight focuses on an analysis and risk recommendations regarding one of the most significant topics affecting the profession: **Telemedicine.**

Terminology

The terms "telehealth" and "telemedicine" are often used interchangeably. However, there are differences:

Telehealth — The Health Resources and Services Administration defines telehealth as "the use of electronic information and telecommunications technologies to support long-distance clinical health care, patient and professional health-related education, health administration and public health." Telehealth generally refers to a broader scope of remote healthcare services, both clinical and non-clinical.

Telemedicine —*Telemedicine* typically refers to a narrower scope of services, namely remote clinical services, including the diagnosis and treatment of patients via telecommunications technologies. While this Spotlight focuses on telemedicine, the broader risk implications for practicing using telehealth are also considered.

Imagine this hypothetical scenario: *A patient who lives in Vancouver, Washington, just across a bridge from Portland, Oregon, chooses to see an NP in Portland near her office. She typically drives to the NP's clinic, but when telehealth visits are available, decides to utilize that option for at least some visits. When the patient comes to the NP's office in Portland, the NP is required only to be licensed in Oregon. However, when that same patient encounters the NP via telehealth from her home in Washington, does that mean the NP must also be licensed in Washington?*

This hypothetical scenario illustrates the type of situations that NPs practicing telemedicine must be prepared to address (especially those NPs whose patient population largely reside near or across state borders). This Spotlight will provide risk management recommendations to help NPs navigate such licensure issues, and address other risks associated with practicing telemedicine.

Risk Management Considerations in Telemedicine

As the provision of healthcare services via technology expands, questions arise regarding the permitted scope of practice, licensure requirements and compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), among other regulatory-based inquiries. It is important for NPs to understand the licensure obligations and risks unique to the practice of telemedicine, as well as risk management best practices, including those related to:

- Verifying competencies and credentials
- Safeguarding patient data
- Communication and documentation
- Coordinating care and monitoring outcomes

The best practices and regulatory guidance regarding the practice of telemedicine are rapidly evolving. It is the shared responsibility of NPs and their employers, where applicable, to know and meet the requirements necessary to provide telemedicine services to their patients. The recommendations outlined in this resource are intended to provide basic information to NPs and to serve as a catalyst for further inquiry into the federal and state regulatory framework for telemedicine/telehealth.

Verifying competencies and credentials

When engaging in telemedicine, it is important for NPs to be cognizant of legal and regulatory requirements. The practice of telemedicine/telehealth occurs where the patient is located at the time the services are provided. Therefore, NPs must hold an active license in the state in which they reside, and they also must be licensed or otherwise authorized to practice in the state in which their patients are located at the time they receive telemedicine services. State requirements vary, and, at times, licensure and practice requirements of multiple states may apply. Resources include the National Conference of State Legislatures, which tracks scope of practice issues related to a range of health care practitioners, encompassing Advanced Practice Registered Nurses (APRNs), as well as the NCSBN APRN Consensus Model Implementation Status Map and Scoring Grid.

The individual practitioner must comply with all applicable state licensing rules and regulations, including nurse practice acts. NPs practicing telemedicine should consider how liability exposure may arise from even seemingly harmless interactions, such as providing routine care, answering patients' or caregivers' questions, or refilling prescriptions. Providing care that exceeds the scope of practice limits is considered practicing without a license and can expose the NP to both civil and criminal liability, as well as licensure discipline, as in the following case study:

Case Study: Practicing beyond the scope of practice; improper billing practices; submitting false claims via telemedicine

In April, the insured NP was issued an APRN license in a new state in order to begin practicing telemedicine in that state while the NP was still physically located in her home state.

The NP began treating diabetic patients via telemedicine, including those covered by the state's public employee insurance plan, and prescribing diabetic supplies and compounded diabetic wound care medications. However, in November, the State Board of Nursing (SBON) received a complaint that some of the NP's patients were receiving expired or incorrectly compounded medications, while other patients were receiving medications labeled for sale only in Mexico and Canada.

Although the NP was not ultimately responsible for the issues with the medications, the SBON's investigation revealed other issues concerning the NP's practice. The SBON found that in the months since the NP obtained an APRN license in the state, the NP had written at least 300 prescriptions to state residents. However, the NP neither applied for nor received prescriptive writing privileges in the state and failed to submit the required documentation to the SBON of a collaborative agreement with an MD or DO. The NP admitted to the SBON that she did not research requirements for prescribing to residents of other states before she began treating patients via telemedicine.

Within weeks of receiving the complaint, the SBON suspended the NP's license, and she ultimately surrendered her license to practice in that state. Over the next year, other SBONs opened their own investigations into the NP's conduct, and she ultimately surrendered her license to practice in at least eight other states. The total incurred to defend the NP in these matters exceeded $25,000.

NPs should consider the following strategies to ensure the ability to practice telemedicine successfully while managing the inherent risks:

- *Gain the necessary skills before initiating telemedicine* by taking focused courses or attending workshops. Research available programs and retain documentation of successful completion of education.
- *Understand all laws and ethical guidelines governing patient interactions, and practice in accordance with the standard of care, the license parameters, and all regulations and ethical guidelines*. NPs practicing telemedicine must adhere to the same practice standards they follow when providing traditional in-person services.
- *Check state and third-party requirements related to telemedicine, licensure, and credentialing,* and, if unsure, contact the SBON for additional information and consult an attorney.
- *Check state requirements related to obtaining, and maintaining, prescriptive authority.* This is an especially important consideration for NPs who may have full practice authority in their state of residence or primary state where they practice who then have to establish a collaborative agreement with a physician, or follow a separate process to obtain prescriptive authority, in another state where their patients are located.
- *Check regulatory board requirements, or if using a third party for reimbursement of telemedicine services, review contractual requirements for patient assessment, coding, and claim submission.* For example, some third parties may require an in-person assessment prior to initiating telemedicine services.
- *Recognize potential issues regarding confidentiality, privacy, cyberstalking, and identity theft.* Use a secure, encrypted platform for communicating with patients. Regularly review, upgrade, or replace equipment or software, as necessary, to meet evolving technology needs and privacy standards.
- *Review relevant regulatory requirements,* including HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act, which govern privacy and security of protected health information (PHI), including electronic transmission. Some states may have higher standards than federal compliance statutes and regulations. Always adhere to the more stringent requirements.

Safeguarding patient data

Providers have a duty to safeguard PHI and prevent unauthorized access to medical records. When engaging in telemedicine, NPs must adhere to medical information and patient privacy requirements of HIPAA, as well as state privacy laws, organizational policies, and ethical standards. To adequately meet HIPAA standards, any electronic systems that transmit or store electronic information regarding patients must be operated and monitored by computer technicians with expertise in security measures. All devices that contain patients' PHI must meet security requirements, and wireless communications must have cybersecurity protection, including end-to-end encryption. All providers and staff members

Telemedicine Liability Self-Assessment Questions

In addition to the technological and clinical concerns that NPs should consider before engaging in telemedicine, they should also weigh the liability risks associated with practicing telemedicine, including:

Offering telemedicine services to patients in a state where the NP is not already practicing

□ Is the NP authorized to practice telemedicine on patients located within that state?

□ What are the state's legal requirements for prescribing?

□ What are the state's legal requirements for informed consent?

□ What technology is permitted?

□ Are there minimum technological/data security requirements?

Extending telemedicine practice to established patients

□ Can telemedicine be utilized for any new concerns, or only for problems initially established during an in-person visit?

□ Are there any prescribing restrictions?

□ Is there a robust informed consent process, in both verbal and written forms?

□ Are billing/payment guidelines understood?

□ Are there contingencies in place in the patient's geographic location in the event of an emergent or urgent situation?

□ What if the patient is located in a different state during the telemedicine encounter? Is telemedicine permitted for established patients?

Extending telemedicine practice to new patients

□ Can telemedicine be utilized for all or only certain kinds of concerns?

□ Are there any restrictions for prescribing?

□ Is there a process for verifying the patient's identity?

□ Is there a robust patient history and informed consent process, in both verbal and written forms?

□ Are billing/payment guidelines understood?

□ Are there contingencies in place in the patient's geographic location in the event of an emergent or urgent situation?

should be educated on how to prevent data breaches when communicating information and transmitting images or audio or video files electronically, and on how to respond when breaches do occur.

NPs should understand that PHI includes more than just patients' medical information. Anything that can identify a patient may be considered PHI, including email addresses, birth dates, telephone numbers, Internet protocol (IP) addresses, among other data elements. NPs also should be aware that state privacy laws may be more stringent than federal regulations. The U.S. Department of Health and Human Services offers tools, guidance documents, and educational materials at HealthIT.gov intended to help providers better integrate HIPAA and other federal health information privacy and security into your practice. The Center for Connected Health Policy (CCHPCA.org) also provides state-specific information on laws, regulations, reimbursement policies, and pending legislation.

In addition to legal requirements regarding PHI during telemedicine visits, NPs must be cognizant of and practice telehealth etiquette. Confirm that the patient has the privacy that they need. Consider who is in the physical space or within listening distance of your discussion when treating patients, including other people who may be in your space, or in the patient's space. Ensure that the patient is aware of any colleagues or staff members who are also participating in the telemedicine visit. NPs should check surroundings and eliminate background noise as much as possible. Place yourself on mute when you are not speaking, and make sure that there is not anything behind you that patients should not see. For further guidance regarding telehealth etiquette, see *"Do you have a good "webside" manner?"* below.

Communication and documentation

Similar to in-person visits, NPs should be cognizant that a signed consent form is merely an acknowledgment that informed consent was previously given. Obtaining legally effective informed consent also requires a verbal discussion of the risks, benefits, and alternatives to the proposed treatment, including a discussion of any patient questions or concerns. These informed consent discussions will vary depending on the patient's complaints and the type of services being rendered. For telemedicine encounters, patients should be clearly informed of the limitations of virtual visits as compared to in-person physical examinations. Patients must understand, acknowledge, and accept the risks associated with the digital care environment. The informed consent process and discussions should be documented in the patient healthcare information record. The Health Resources & Services Administration developed a list of recommendations and resources to guide organizations and providers in obtaining informed consent.

As part of the informed consent discussion for telemedicine, patients should be informed that the provider has the discretion to determine whether telemedicine is appropriate for the encounter or if an in-person visit is needed, based upon circumstances including the patient's complaint and presentation. Many factors can influence a patient's ability to interact effectively with the provider via telemedicine, including disability, age, access to equipment and adequate bandwidth, and familiarity with technology. According to The American Telemedicine Association (ATA), "It should be the responsibility of the provider to escalate to a higher level of care (or otherwise initiate appropriate recommendations) when medically indicated or necessary for patient safety." This protocol will help to ensure that the patient's expectations are realistic and that they will be compliant with any recommendations for an in-person care. In cases of a patient declining to follow the recommendation for an in-person visit, their informed refusal should be documented appropriately in the patient's healthcare information record.

NPs should document telemedicine in the patient's healthcare information record in accordance with their organization's standards for in-person care. In general, telemedicine documentation should include, in accordance with state and federal regulations:

- Patient name.
- Patient identification number at originating site (if applicable).
- Provider organization's name.
- Date of service.
- The specific interactive telecommunication technology used for the visit.
- Reason(s) the visit was conducted using telecommunication technology, rather than face-to-face.
- Type of evaluation to be performed.
- Informed consent documentation.
- Evaluation results.
- Diagnosis/impression of practitioners.
- Recommendations for further treatment.
- All communications with the patient (whether verbal, audiovisual, or written).
- Follow-up instructions and any referrals to specialists.

For further guidance regarding documentation, refer to the Nurse Practitioner Spotlight: Healthcare Documentation.

Coordinating care and monitoring outcomes

Telemedicine presents certain advantages to traditional, in-person care, including enabling the NP to view the patient in the home environment, engage with members of the patient's care team who may be geographically distant, and potentially permit more uninterrupted discussion with the patient. Nevertheless, it can be especially challenging to establish and meet evidence-based standards in the telemedicine environment due to potential data transmission issues. In a telemedicine visit, clinical decision-making depends upon patient self-reporting of symptoms, which may include the utilization of clinical biometric data from remote patient monitoring devices. User errors and internet bandwidths and speeds can affect the validity and reliability of patient assessments, which in turn can result in healthcare providers making clinical treatment decisions based upon potentially inaccurate patient data. Moreover, traditional physical examination techniques, such as abdominal exams or fine motor task measurements, are not possible, and alternative techniques may be required. In the absence of these key sources of data, the diagnostic process may need to be deferred until all diagnostic test results are available, which may include a physical examination. Organizations must develop clear escalation protocols so that patients who relay abnormal biometric data or test results are appropriately referred for higher levels of care.

NPs should remember that diagnostic errors are a prevalent patient safety issue and the top area of liability for NPs, as evidenced in the Nurse Practitioner Liability Claim Report: 5th Edition, as well as the Nurse Practitioner Spotlight: Diagnosis. As clinicians, NPs bear the ultimate responsibility for determining when to terminate telemedicine visits and require that the patient come into the office or seek emergency care. Due to the patient safety implications, NPs should consider when the risk of a diagnostic error is too high, and an in-person visit is required.

Protocols should be implemented to ensure that patients have appropriate follow-up appointments and instructions for pending diagnostic testing. NPs also should consider that just because they send their patient a message or push notification via a patient portal, that does not necessarily ensure that the patient read the message, understood it as the provider intended, and knows what next steps to take. Therefore, follow-ups and closing the communication loop are critical. For example, utilizing closed loop specialist referrals can help ensure that the patient follows up with specialists for testing and helps the NP follow the patient's treatment. For NPs who provide services primarily through telemedicine, and who may not have an ongoing relationship with the patient, these types of protocols are imperative. Furthermore, inappropriate termination of care or becoming inaccessible to the patient may result in abandonment allegations. A protocol for referring the patient to a hospital emergency department or urgent care clinic should be created and utilized in the event that a patient experiences an emergency during the telemedicine encounter, and/or they are unable to contact the telemedicine provider.

NPs must be conversant with the use of all remote monitoring devices and remote physical examination techniques that may be utilized during patient encounters in advance of scheduling any telemedicine visits with patients. Educational resources for remote physical examination techniques are available through Stanford Medicine, the California Telehealth Resource Center, the Department of Health and Human Services and the National Institute of Health.

Nurse Practitioner Spotlights

For risk control strategies related to:

- Defending Your License
- Depositions
- Documentation
- Patient Adherence
- Diagnosis
- Prescribing

Visit nso.com/npclaimreport

References and Additional Resources

- American Nurses Association (ANA): ANA Core Principles on Connected Health/Telehealth. https://www.nursingworld.org/get-involved/share-your-expertise/pro-issues-panel/connected-health-telehealth/

- American Association of Nurse Practitioners (AANP). Position Statement: Telehealth. https://www.aanp.org/advocacy/advocacy-resource/position-statements/telehealth

- Balestra, M. (2018). Telehealth and legal implications for nurse practitioners. *The Journal for Nurse Practitioners*, *14*(1), 33-39. https://www.npjournal.org/article/S1555-4155(17)30808-5/fulltext

- Butzner, M, & Cuffee, Y. (2021). Telehealth interventions and outcomes across rural communities in the United States: narrative review. Journal of medical Internet research, 23(8), e29575. https://www.jmir.org/2021/8/e29575/

- Center for Connected Health Policy – National Telehealth Policy Resources Center. https://www.cchpca.org/

- Gajarawala, SN, & Pelkowski, JN. (2021). Telehealth benefits and barriers. *The Journal for Nurse Practitioners, 17*(2), 218-221. https://www.npjournal.org/article/S1555-4155(20)30515-8/fulltext

- HealthIT.gov. Health IT Privacy and Security Resources for Providers. U.S. Department of Health and Human Services. https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers

- Hood, C, Sikka, N, Manaoat Van, C, Mossburg, SE. (2023). Remote Patient Monitoring. PSNet. Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services. https://psnet.ahrq.gov/perspective/remote-patient-monitoring

- Mechanic OJ, Persaud Y, Kimball AB. Telehealth Systems. 2020 Sep 18. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2021 Jan–. PMID: 29083614. https://www.ncbi.nlm.nih.gov/books/NBK459384/

- National Conference of State Legislatures. (2023). Scope of practice policy: Advanced practice registered nurses. https://scopeofpracticepolicy.org/practitioners/advanced-practice-registered-nurses/

- Perry AF, Federico F, Huebner J. (2021). Telemedicine: Ensuring Safe, Equitable, Person-Centered Virtual Care. IHI White Paper. Boston: Institute for Healthcare Improvement. https://www.ihi.org/resources/white-papers/telemedicine-ensuring-safe-equitable-person-centered-virtual-care

- Sinsky CA, Jerzak JT, Hopkins KD. Telemedicine and Team-Based Care: The Perils and the Promise. Mayo Clin Proc. 2021 Feb;96(2):429-437. doi: 10.1016/j.mayocp.2020.11.020. PMID: 33549262; PMCID: PMC7857703. https://www.mayoclinicproceedings.org/article/S0025-6196(20)31379-3/fulltext

- U.S. Department of Health and Human Services – Telehealth Dashboard for Providers. https://telehealth.hhs.gov/providers

- U.S. Department of Health and Human Services. (2022). Obtaining Informed Consent. Health Resources & Services Administration. https://telehealth.hhs.gov/providers/preparing-patients-for-telehealth/obtaining-informed-consent/

- Weaver, MS, Lukowski, J, Wichman, B, Navaneethan, H, Fisher, AL, & Neumann, ML. (2021). Human Connection and Technology Connectivity: A Systematic Review of Available Telehealth Survey Instruments. Journal of pain and symptom management, 61(5), 1042–1051.e2. https://doi.org/10.1016/j.jpainsymman.2020.10.010

Do you have a good "webside" manner?

Delivery of care using telemedicine techniques may create significant benefits, including the ability to reach underserved or rural communities, and bypassing obstacles that may limit or prevent individuals from accessing care face-to-face. A telemedicine visit may feel very different to a patient, especially patients with limited experience using technology. However, the following steps will help improve the experience for both you and your patients.

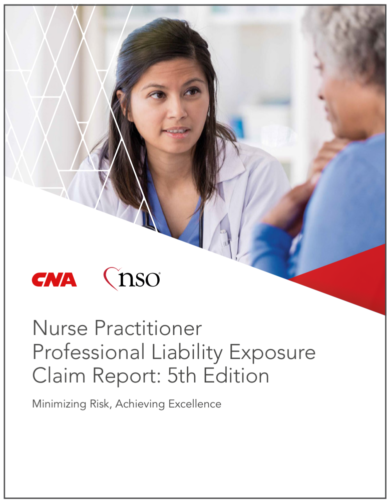
Before the visit:

- □ Ensure that you are at ease with the telemedicine technology. If necessary, ask another staff member to be available in case you encounter any issues.
- □ Eliminate any background distractions and find a space with adequate lighting. If possible, conduct visits in an area where you are facing a source of natural light.
- □ Clarify the telehealth services being offered and incorporate patient preferences, where possible (for example, an audio-only versus an audiovisual visit).
- □ Validate that the patient can establish a clear connection. Provide the patient with guidance on how to use the technology (for example, a handout or pre-recorded video link).
- □ Ensure that the patient has information on how to address possible technical issues and what to do if they encounter technology issues.
- □ Encourage patients to plan a quiet, private, and comfortable place to set themselves up for the visit, which may not be possible in all cases.
- □ Offer and arrange for interpretive services, when necessary, to account for the patient's preferred language or communication method.

During the visit:

- □ Verify the patient's identity and the reason for the visit.
- □ Respect patient privacy, including being cognizant that you may be viewing the patient's home.
- □ Look into the camera, when possible, to simulate eye contact.
- □ Listen actively and empathetically.
- □ Inform the patient when you are documenting or taking notes, so they know why you are looking away from the screen.
- □ Maintain a normal pace of speech, speaking slowly and enunciating so that the patient can understand you.
- □ When you're listening, be aware of your resting facial expression.
- □ Use patient education tools, such as the teach back method, to ensure patient understanding.
- □ Engage the patient's care partners in telemedicine appointments and patient education, such as spouses or family members, when appropriate and only with the patient's explicit consent.
- □ Before ending the encounter, verify that you have addressed all patient questions and concerns and that the patient verifies understanding of any follow-up steps that must be completed.
- □ Plan any appropriate follow-up communications with the patient. Consider whether automated reminders/push notifications deployed via a patient portal are sufficient, given the patient's unique circumstances and characteristics, or if a follow-up phone call or visit is warranted.

This tool provides a reference for nurse practitioners seeking to evaluate basic risk exposures. 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 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 compassing a review relevant laws and regulations. CNA assumes no responsibility for the consequences of the use or nonuse of this information.



CNA nso

Nurse Practitioner
Professional Liability Exposure
Claim Report: 5th Edition

Minimizing Risk, Achieving Excellence

This information was excerpted from NSO and CNA's full report, *Nurse Practitioner Liability Claim Report: 5th Edition*. www.nso.com/NPclaimreport

1100 Virginia Drive, Suite 250
Fort Washington, PA 19034
1.800.247.1500 www.nso.com

151 N. Franklin Street
Chicago, IL 60606
1.888.600.4776 www.cna.com

In addition to this publication, CNA and Nurses Service Organization (NSO) have produced numerous studies and articles that provide useful risk control information on topics relevant to nurses, as well as information relating to nurse insurance, at www.nso.com. These publications are also available by contacting CNA at 1-866-262-0540 or at www.cna.com. 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 registered trademark of CNA Financial Corporation. Certain CNA Financial Corporation subsidiaries use the "CNA" trademark in connection with insurance underwriting and claims activities.

Nurses Service Organization (NSO) is the nation's largest administrator of professional liability insurance coverage to nurses. For more information about NSO, or to inquire about professional liability insurance for nurses, please contact NSO at 1.800.247.1500 or visit NSO online at www.nso.com.

Nurses Service Organization is a registered trade name of Affinity Insurance Services, Inc. (TX 13695); (AR 100106022); in CA, MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services, Inc.; in CA, Aon Affinity Insurance Services, Inc. (CA 0G94493); Aon Direct Insurance Administrators and Berkely Insurance Agency; and in NY, AIS Affinity Insurance Agency.