Rapid technological advances over the last few decades have changed healthcare in ways that were never possible or imagined in the past. Perhaps one of the most compelling aspects of this advancement is technology’s ability to transcend time and distance. With the click of a button, information can be sent at high speeds over many miles, increasing both efficiency of, and access to, care.

With these advances, the concepts of telemedicine and teledentistry have evolved. In years past, these terms often referred to healthcare consultations that occurred over landline telephones. Now, both the technology and terminology have expanded.

Landline telephones are no longer the sole mode of information transmission. Providers now use various methods to send and retrieve data, including web technologies, wireless networks, satellites, and more.

Further, although “telemedicine” and “teledentistry” are still part of the common vernacular, a broader term — “telehealth” — has come into usage as well. Telehealth describes the use of telecommunication technology to exchange health information from one site to another for the purpose of clinical services, public health, oral health, eye care, allied health, and both patient and provider education.¹

Although a general consensus has not been reached on the exact definitions of these terms — and legal and regulatory standards may differ based on how governing bodies define the terms — for the purposes of this article, “telehealth” is used to encompass both telemedicine and teledentistry activities.

Why Telehealth?

With today’s increasing pressure on healthcare providers to improve quality of patient care and cut costs, the emphasis on telehealth is becoming more pronounced, and the ways in which it is used are expanding.

Both the dental and medical communities have recognized telehealth as an up-and-coming area of practice. In 2011, the American Dental Association’s House of Delegates adopted a resolution that directed its Council on Dental Practice to spearhead an evaluation of teledentistry in dental practices.²
In 2012, the Institute of Medicine explained that the role of telehealth is becoming more important “as we move away from the traditional fee for service system and toward new models of care, including accountable care organizations (ACOs), patient-centered medical homes (PCMHs), and other strategies that focus on outcomes.”

Additionally, proponents of telehealth cite a number of potential benefits, including:

- Improved access to care and resources for patients in rural areas or areas that have provider shortages
- Lower costs and improved efficiency as a result of pooling resources, reducing travel time, and better managing patient care
- Comparable or improved quality of care
- Increased patient satisfaction, which may occur as a result of better access to care, convenience, and reduced stress

**How Is Telehealth Regulated?**

Like many other aspects of healthcare, telehealth is regulated at both the federal and state levels. A number of government agencies may be involved in determining legal parameters for telehealth, including the Food and Drug Administration (FDA), the Centers for Medicare & Medicaid Services (CMS), and the Drug Enforcement Administration (DEA).

The National Telehealth Policy Resource Center, a program of the Health Resources and Services Administration (HRSA), notes that as mobile technologies emerge, additional federal agencies will likely have jurisdiction, including the Federal Trade Commission (FTC), Federal Communication Commission (FCC), and the Department of Health and Human Services (HHS).

State legislatures and state medical and dental boards also play a significant role in determining telehealth standards and boundaries within individual states, including licensure requirements, scope of practice parameters, and issues concerning reimbursement.
Although the use of telecommunications in healthcare is not new, it is only now becoming more widespread. Thus, many states may not yet offer specific laws or detailed guidance on telehealth activities. As telehealth becomes more common, providers can expect to see more defined state and federal policies.

What Are the Risks and Barriers Associated With Telehealth?

The delivery of healthcare via telecommunication technology presents healthcare providers and organizations with unique risks and challenges. Some of the main areas of concern are licensing, credentialing/privileging, online prescribing, informed consent, and the privacy/security of confidential health information.

Licensing

Although technology has created opportunities for physicians, dentists, and other healthcare providers to extend their reach beyond the physical limitations of their geographic location, it does not transcend the boundaries of state law. Therefore, a discussion about the risks associated with licensing largely hinges on variations in state statutes and regulations.

While some states offer direct guidance related to the practice of telehealth, others provide limited information or do not address the issue at all. Even when state laws do address telehealth, they can differ significantly from state to state. For example, states may:

- Require full licensure for telehealth practice
- Offer an abbreviated telehealth licensing process
- Allow out-of-state doctors to provide telehealth services within the state without obtaining a license (as long as the doctor has a valid license in another state)

Further, some states have exceptions to their laws, such as for consultations.\(^6\) A 2009 white paper from the American Health Lawyers Association notes that in the absence of state guidance, doctors can likely assume that they need a license in the state where the patient is located. Additionally, doctors practicing within the boundaries of one state should verify licensing laws, because some states require special telehealth licenses or permits.\(^7\)

Healthcare providers and organizations participating in telehealth programs should be cognizant of state telehealth laws, practice acts, and standards of care for each state in which they plan to practice. Even if providers don’t plan to have a physical presence in the state, long-arm laws may grant state courts jurisdiction over out-of-state individuals whose actions have potentially harmed a local resident.\(^8\)

To learn more about the statutes and regulations in the state(s) in which you practice, visit http://cchpca.org/state-laws-and-reimbursement-policies or contact the state’s medical board or dental board.
Credentialing and Privileging

Credentialing and privileging — the processes by which an organization or practice assesses and confirms the qualifications of a healthcare provider and authorizes the provision of specific services — play an important role in patient safety and quality care. This is equally true for both traditional, in-person care and telehealth services.

The ECRI Institute explains that while remote practitioners will not have the same relationship with a healthcare facility as do onsite providers, the facility still must exercise the same level of due diligence in its screening and selection processes. They must ensure that the distant site practitioner is legally allowed to provide care to the specified patient population, and that he or she is qualified for the scope of services requested.

Since 2011, CMS has allowed the governing body of an organization whose patients are receiving telehealth services to rely on credentialing and privileging decisions made by a distant site hospital or “telemedicine entity,” such as a teleradiology group or ambulatory surgery center. This is known as “credentialing by proxy.” Credentialing by proxy helps organizations save time and money, but certain requirements must be met, such as a written contract between the originating and distant sites. For more information, visit http://cchpca.org/credentialing-and-privileging.

In addition to federal credentialing and privileging standards, states, accrediting bodies, certifying organizations, and third-party payers also may have credentialing and privileging standards related to telehealth. Providers and organizations engaged in telehealth activities and programs should be aware of the requirements that apply to them.

Online Prescribing

Online prescribing refers to a “provider’s ability to prescribe drugs to a patient who has been diagnosed and treated via telehealth.” Online prescribing is different from e-prescribing, which simply refers to a provider’s ability to send prescriptions electronically to a pharmacy, but does not account for whether the patient was seen in person or using telecommunication technology.

Technology has, in certain circumstances, eliminated the need for the face-to-face visits that are typical in traditional medical and dental care. However, when it comes to prescribing medications, lack of physical interaction creates patient safety and liability concerns.

In fact, the Center for Telehealth & e-Health Law notes that “the majority of legal actions that have been brought against telehealth providers proceeded as a result of telemedicine practitioners prescribing medications over the internet, rather than actions having been brought because care was negligently administered through telemedicine.”
Major concerns related to online prescribing include whether an appropriate provider–patient relationship has been established, whether the doctor has been able to adequately assess the patient, and whether the patient has provided an accurate health history.

Doctors who plan to prescribe medications as part of telehealth services should be aware of both federal and state prescribing regulations.

**Federal Prescribing Regulations**

CMS addresses e-prescribing as part of its Medicare rules, and the DEA addresses online pharmacies and telemedicine as part of the Controlled Substances Act. Further, the 2008 Ryan Haight Online Pharmacy Act — named for a teenage boy who died after overdosing on pain medication prescribed by a doctor whom he had never seen — prohibits the distribution of controlled substances via the Internet in the absence of a valid prescription. The validity of a prescription is based on whether a practitioner examined the patient in person, “with certain exceptions for telemedicine activities.”

**State Prescribing Regulations**

State regulations regarding online prescribing vary from state to state and may or may not include guidance for in-person evaluation, establishment of a doctor–patient relationship, written protocols, etc. Thus, doctors should consider whether states in which they practice:

- Put restrictions on how the provider–patient relationship is defined
- Require doctors to have a preexisting relationship with the patient in order to engage in online prescribing
- Require a face-to-face physical exam prior to online prescribing, and whether the exam can be performed using a telehealth medium, such as videoconferencing
- Prohibit questionnaires and surveys as the sole basis for online prescribing
- Have other requirements related to patient medical history, written documentation, appropriate follow-up care, and emergency provisions

---

**Case Example**

In a case involving online prescribing, a doctor in state A, who worked as a subcontractor for an online pharmacy, prescribed an antidepressant to a patient living in state B. The patient initiated the request through an off-shore website by filling out a questionnaire, which was then forwarded to a processing firm in state C. The processing firm, in turn, sent the request to the physician.

The doctor reviewed the questionnaire and submitted an online prescription for the antidepressant. A pharmacy in state D filled the prescription and shipped it to the patient. During the course of this process, the doctor never met or communicated directly with the patient. Shortly thereafter, the patient committed suicide.

Charges were brought against the doctor for practicing medicine in state B (the patient’s home state) without a license. The doctor sought to have the charges dropped on the basis of lack of jurisdiction. However, the court determined that the doctor was subject to personal jurisdiction in state B, even though he was never physically present in the state.

The doctor ultimately pleaded no contest to the felony charge; he was sentenced to 9 months in county jail and ordered to pay more than $4,000 to the court and state B’s medical board.
State-specific information about online prescribing can be obtained from state medical and dental boards. For general information about online prescribing, visit the National Telehealth Policy Resource Center at http://cchpca.org/online-prescribing-0 or the Telehealth Resource Centers at http://www.telehealthresourcecenter.org/toolbox-module/online-prescribing-and-telepharmacy.

**Informed Consent**

Informed consent — a process that is used to educate patients about the potential benefits, risks, and alternatives to a proposed treatment — is a crucial component of a patient’s right to make decisions about his or her healthcare.

MedPro Group’s *Informed Consent* guideline explains that “any procedure that presents the possibility of material harm to a patient should not be undertaken until the informed consent process has been completed. The thoroughness and complexity of the informed consent process will depend on the degree of risk that accompanies the procedure.”

The importance of informed consent applies to telehealth just as it does to traditional care. However, in telehealth, the informed consent process must also take into account risks specific to the delivery of care using telecommunication technologies.

A recent article about informed consent and telehealth states that “in the practice of telehealth, reliance on imperfect technological tools, as well as the ‘distance’ factor, can propel otherwise routine treatments into a higher risk category.” Risks specific to telehealth include technological glitches and failures (including transmission errors), technology-related privacy and security concerns, and lack of hands-on patient evaluation.

As telehealth has become a more viable option for healthcare delivery, a handful of states have implemented informed consent laws that pertain specifically to telehealth. As with licensure, informed consent laws vary between states. For example, some states may require written informed consent, while others permit verbal consent.

Even in the absence of state guidance, telehealth providers should carefully consider their use of an informed consent process. As the aforementioned article notes, “failure to properly obtain a patient’s informed consent before initiating telehealth services can increase a provider’s risk of facing consent-based negligence claims . . .”

Whether developing a separate informed consent process or modifying an existing process to cover telehealth, providers may want to include (in addition to all standard and state-required informed consent information):

- The names of all involved healthcare providers and their credentials and locations, as well as any other staff that may help facilitate the telehealth service
- A description of the telehealth service that will be performed and the technology that will be used
- Alternative options for treatment and care
- Any risks specifically related to the electronic nature of the care delivery (e.g., technology disruptions, failures, or limitations)
- Specific security and privacy measures that have been implemented, as well as any increased privacy risks relative to the telehealth technology
- A plan for ongoing care, including details about who is responsible for various aspects of the patient’s care
- A plan for alternative care in the case of an emergency or technological malfunction

All providers involved in the telehealth program should have a clear understanding of the informed consent process, and — as with traditional informed consent — the process should be documented in the patient’s record.

**Privacy/Security**

The rapid expansion of technology in healthcare has significant implications for privacy and security of patient’s protected health information (PHI). Even in the absence of telehealth services, electronic information creates security issues (such as the increased risk of loss or theft of mobile devices, like laptops and flash drives). When telecommunications is thrown into the mix, the issue becomes even more complex.

For example, the transmission of data to and from various locations increases the risk of inappropriate disclosure and data breaches. Thus, healthcare practices and organizations must implement privacy and security safeguards at all points of exposure, including at the originating site, across the transmission medium, and at the distant site. Examples of these safeguards include data encryption, user authentication, password security, patient verification technologies, protected wireless networks, data tracking and auditing, and more.

Further, telehealth activities must comply with federal HIPAA privacy and security standards, as well as any state laws related to privacy and security of health information.

Specifically, the HIPAA omnibus rule that was published in January 2013 sets forth standards related to electronic PHI and requires covered entities and business associates to implement policies and procedures “to prevent, detect, contain, and correct security violations,” inclusive of risk analysis and risk management activities.

When working with vendors who supply telehealth services or equipment, healthcare practices and organizations should determine whether the vendors are considered business associates per HIPAA standards. A business associate “is a person who . . . creates, receives, maintains, or transmits protected health information for a function or activity regulated by [45 CFR, Subtitle A, Subchapter C].”
If a vendor qualifies as a business associate, the practice and vendor should have a business associate agreement (BAA) in place. The agreement should outline appropriate use and disclosure of PHI by the vendor to ensure security. For more information about business associates and a sample BAA, visit http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Healthcare practices and organizations also should consider their policies related to security of mobile devices, use of social media, appropriate technologies and applications (apps), and electronic communication with patients. A risk analysis that takes into account the services offered, the method of delivery, and the types of technologies involved can help practices identify areas of exposure and take action to address them. For additional guidance on risk analysis requirements under HIPAA, visit http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

Additionally, all providers and staff involved in telehealth activities — including support staff, technical staff, vendors, etc. — should be aware of their obligation to protect patient confidentiality and adhere to privacy and security laws. Periodic training on information privacy and security, as well as use of confidentiality agreements, can help reinforce compliance with the practice’s protocols.

**What Are the Malpractice Trends Related to Telehealth?**

Issues surrounding telehealth and malpractice liability are complex and not yet well defined, as the expansion of telehealth in medical and dental care is relatively recent.

Robert L. Ignasiak, Senior Vice President and Claims Leader at MedPro Group, notes that “To date, we have not seen many telehealth cases driven by technology itself, but rather from causes that just as well might occur in the absence of telehealth, such as communication failures and documentation issues.” To address these issues, he explains, physicians and dentists must ensure that the “same discipline they follow in treating patients in person also applies to patients being treated or evaluated remotely.”

In addition to managing general risk concerns, practitioners may face other uncertainties specifically related to the provision of care via telecommunications. For example, because standards and regulations for medical malpractice vary by state, telehealth programs and services that cross state lines may create legal concerns pertaining to jurisdiction, procedure, choice of state law, and standards of care. 

---

**Are You Covered?**

When starting a telehealth program or considering participating in telehealth initiatives, it's important to know whether your professional liability insurance provides coverage for these activities. Your insurance agent or broker can help answer questions about policy coverage for telehealth services. If you do not have an agent or broker, contact your professional liability carrier and ask for assistance with this coverage issue.
Further, the ECRI Institute notes that lawsuits involving telehealth “are more likely to target numerous defendants and involve more than one theory of liability.”24 A telehealth-related lawsuit may name providers at the originating and distant sites, as well as their healthcare facilities, as defendants. A lawsuit also could potentially implicate telecommunication vendors and their consultants.

To help mitigate the risks associated with telehealth and medical liability, providers should carefully consider:

- The locations in which they are providing services
- Any relevant state malpractice laws, licensure regulations, and standards of care
- The actions that may trigger a doctor–patient relationship
- Whether arrangements and contracts with telehealth partners explicitly state provider responsibilities for ongoing care and follow-up
- State and federal fraud and abuse regulations (such as the Anti-Kickback Statute and Stark law)
- Whether all parties involved in the telehealth program or service have appropriate professional liability coverage

For more information, visit the Telehealth Resource Centers’ Legal and Regulatory Module at http://www.telehealthresourcecenter.org/legal-regulatory.

As the use of telecommunications in the delivery of care becomes more prominent, doctors can reasonably assume that litigation associated with telehealth services will also increase, leading to more defined malpractice patterns and trends.

**Conclusion**

Advances in telecommunication technologies have the potential to revolutionize healthcare delivery and help address burgeoning issues related to cost, accessibility, and quality of care. Yet, as providers venture into the emerging realm of telehealth, they should be cautious and aware of the potential risks these new technologies present.

Major areas of risk concern for telehealth include licensing, credentialing and privileging, online prescribing, informed consent, and health information privacy and security. By considering these areas in the context of telehealth, practitioners and organizations can identify safety and liability issues and proactively implement safeguards.
### Top 10 Risk Strategies for Telehealth

1. Be aware of federal and state laws and regulations related to telehealth, such as requirements for licensure, online prescribing, informed consent, clinical decision-making, and quality improvement. Check with your state medical or dental board for specific guidance.

2. Identify and implement telehealth best practices, and stay abreast of any changes in telehealth regulations and standards of care. The American Telemedicine Association and other professional associations have published a number of telemedicine practice guidelines.

3. Ensure that telehealth providers at remote sites are properly credentialed (either by the originating site or the distant site) and qualified for their proposed scope of services. Any privileges granted should comply with applicable scope of practice laws.

4. Develop and implement patient selection criteria and standardized clinical protocols as appropriate to ensure consistency, quality, and efficiency of telehealth services.

5. When multiple providers are involved in a patient’s care, have a clear understanding of duty of care and clinical responsibilities, including disclosure of any adverse events. Make sure the specific provisions are documented.

6. Implement protocols to ensure that communication from telehealth providers is promptly reviewed and acted upon.

7. Ensure that technology and equipment used for telehealth services is functional and properly maintained and serviced. Providers and staff should be aware of who is responsible for equipment maintenance.

8. Assess the privacy and security risks of your telehealth systems, and implement safeguards at all points of risk exposure. Monitor the systems for possible security breaches.

9. Train telehealth providers and staff on applicable telecommunication technologies, scope of telehealth services offered, equipment maintenance, and privacy/security standards.

10. Ensure that the organization’s mechanism for incident reporting supports telehealth events, and evaluate telehealth activities as part of ongoing quality improvement initiatives. Surveys or questionnaires can help gauge provider and patient satisfaction with telehealth services.

### Endnotes


10 ECRI Institute, Telemedicine.


13 Natoli, Summary of findings: Malpractice and telemedicine.


19 Scott, Proactively approaching telehealth informed consent.

20 ECRI Institute, Telemedicine.

21 HIPAA Privacy and Security Rule, 45 C.F.R. § 164.306.

22 HIPAA Privacy and Security Rule, 45 C.F.R § 160.103.


24 ECRI Institute, Telemedicine.

The information provided in this document should not be construed as medical or legal advice. Because the facts applicable to your situation may vary, or the regulations applicable in your jurisdiction may be different, please contact your attorney or other professional advisors if you have any questions related to your legal or medical obligations or rights, state or federal statutes, contract interpretation, or legal questions.


© MedPro Group.® All Rights Reserved.