

connection

PROFESSIONAL SOLUTIONS INSURANCE COMPANY BRINGS YOU PRACTICAL TIPS FOR AVOIDING A MALPRACTICE ALLEGATION

ISSUE 4 • 2014



Telemedicine—Seeing Isn't Always Believing

In telemedicine, all is not what it appears to be. What constitutes a physician/patient relationship is at the core of legal issues in this area.

By Linda J. Hay & Susan A. Wagener

Over the course of his 25-year career, John Frankzen, M.D., had an obstetrical/gynecological practice and later an administrative role at a large multi-specialty clinic. During this time, Dr. Frankzen had no discipline issues related to his license.

Looking to transition to a less hectic position, Dr. Frankzen then took a position as an independent contractor/consultant in January 2007 with Safe Medicine. His duties were to include prescribing medications to patients across the country.

At that time, there were no specific federal regulations governing telemedicine. Nonetheless, Dr. Frankzen raised the issue of requirements with Safe Medicine.



Safe Medicine advised that patients would be required to have had a physical examination by a licensed physician within the past 24 months, and all records would be provided to Dr.

Frankzen for his review. Prior to dispensing any medications, Dr. Frankzen would then consult with the patient by phone. However, he would not conduct physical examinations of patients nor meet with them face to face.

Safe Medicine advised Dr. Frankzen that the company had four requirements for prescribing medications:

1. The patient had a legitimate medical complaint.
2. A comprehensive medical history had been obtained.
3. A physical exam had been obtained (not necessarily by the prescribing physician) and records documented this.
4. There was a logical connection between the medical complaint, medical history, physical exam and drug prescribed.

Dr. Frankzen Requests Legal Evaluation

Dr. Frankzen, concerned about his bounds as a licensed physician, requested that the company provide him with a legal evaluation of what he could and could not do in accordance with the standard of care.

The company shared documents detailing the standard of care for the telemedicine consulting program, as well

The goal of *Physician Connection* is to feature articles by leaders in the medical, legal and risk management professions, and we believe you'll enjoy the in-depth perspectives shared by our authors. We realize the practice of medicine is an art and not a science. A patient's medical history and treatment plan should be based on both the patient's condition and the physician's clinical opinion. Therefore, the views and opinions expressed are those of the authors and do not reflect the policy or position of PSIC.

as an analysis of the DEA's law and policy for telemedicine practices.

Around this time, federal regulations were becoming more specific. Safe Medicine's legal personnel advised that its company policies and procedures appeared to be consistent with the intent of the proposed Ryan Haight Online Pharmacy Consumer Protection Act. They also believed the company was compliant with all other telemedicine standards.

Confident that the company's legal team had performed a thorough analysis and that its policies and procedures addressed federal and state requirements, Dr. Frankzen accepted the position. Therefore, he began prescribing medications to patients he had never met or evaluated. Some of those medications included controlled substances, such as hydrocodone, for patients with longstanding histories of ailments, such as back pain.

Dr. Frankzen did not, however, independently review his state's medical licensing act. In fact, he hadn't reviewed it in many years.

Continued on Page 2

As telemedicine gains a stonger foothold, some of the issues will begin to resolve.

In 2008, federal regulations (specifically the Ryan Haight Online Pharmacy Consumer Protection Act of 2008) were adopted that formally changed the climate of telemedicine. Safe Medicine's legal department, on its own accord, provided Dr. Frankzen with an updated analysis of the DEA's law and policies for telemedicine. The company's legal department advised Dr. Frankzen that the company's policies and procedures were consistent with the intent of the Ryan Haight Online Pharmacy Consumer Protection Act of 2008 and other telemedicine medical standards.

Dr. Frankzen felt that Safe Medicine was just as concerned as he was about ensuring the practices were legal. Safe Medicine had a vested interest in abiding by the law and had devoted considerable legal resources to staying on top of the law's constant changes. As such, Dr. Frankzen felt he could rely upon their opinions, and he continued to practice with Safe Medicine.

Dr. Frankzen Concerned; Makes Transition

The landscape of what constituted a physician/patient relationship was being redefined through federal telemedicine laws and regulations in April 2009. These required the prescribing physician to have a face-to-face encounter with the patient before prescribing a controlled substance.

This change, in Dr. Frankzen's view, was contrary to his practice at Safe Medicine because the company's protocol did not allow for the type of patient encounter now required by law.

Accordingly, he left Safe Medicine in April 2009. Indeed, the changes proved impossible for both Safe Medicine and Dr. Frankzen to overcome. Safe Medicine went out of business in 2009.

Dr. Frankzen took an administrative position with a company involved with corporate health plans where he would interpret and draft policies. In this position, he would no longer treat individual patients or prescribe medications.

Board Allegations Ensur

In 2010, Dr. Frankzen received a notice from his state disciplinary agency asserting he had violated the state's Medical Practice Act. At an informal conference held with the agency representative, Dr. Frankzen and his counsel shared the facts of the case.

Dr. Frankzen provided extensive documentation from Safe Medicine



regarding their research and interpretation of applicable law. Unfortunately, the agency disagreed with Safe Medicine's conclusions, and they recommended license suspension. Dr. Frankzen did not agree with that recommendation.

The matter then moved to a more serious phase of the disciplinary process. A complaint was filed alleging that Dr. Frankzen:

1. Regularly authorized prescriptions for medications including controlled substances while working with Safe Medicine.
2. Did not physically examine any of the persons to whom he prescribed medications.

3. Had no physician/patient relationship with the persons receiving these prescriptions because they had not met with Dr. Frankzen physically.

Accordingly, the complaint alleged Dr. Frankzen breached the accepted medical standard of practice. Eighteen specific patient prescriptions for 18 different patients were identified in the complaint.

Dr. Frankzen denied the allegations and provided additional materials and research to the disciplinary agency. Dr. Frankzen and his lawyers emphasized the fact that the law was unsettled at the time of the allegations, and Dr. Frankzen's current position did not involve direct patient care or writing prescriptions.

Board's Decision

While sensitive and sympathetic to these factors, the agency felt discipline was necessary both for individual reasons (Dr. Frankzen's failure to independently analyze the requirements) and policy reasons, given the surge of issues related to telemedicine.

After further assessment and review, the disciplinary agency's lawyers proposed a three-month license suspension, 25 hours of continuing education on medical ethics and a \$2,000 fine. Dr. Frankzen agreed to these terms. Dr. Frankzen's attorney's fees were approximately \$15,000.

What Can We Learn?

Dr. Frankzen believed he had reasonably relied on Safe Medicine's legal department's analysis of changes in the law and prescribed medication accordingly. Unfortunately, Safe Medicine's analysis and opinions were rejected by the disciplinary agency. In hindsight, Dr. Frankzen might have conducted an independent review of Safe Medicine's protocols and opinions as a check and balance. He could have

done this by retaining his own counsel, contacting his malpractice insurance carrier or using other resources in the medical community.

That independent review may have provided support to the disciplinary agency that Dr. Frankzen did not blindly rely on a for-profit entity's evaluation to justify actions that were outside of the scope of the Medical Practice Act. Had Dr. Frankzen done so before accepting the job, it likely would have helped his defense.

Though not easy, physicians who rely on telemedicine must keep current on laws, statutes and acceptable practices. An excellent resource is the American Telemedicine Association (www.americantelemed.org). The National Institute of Health (www.nih.gov) and Centers for Medicare and Medicaid (www.cms.gov) also provide helpful resources.

It's critically important to review state medical practice acts yearly for updates and changes. Regular review of these materials will help shape what is considered acceptable medical practices from a liability perspective. If a statute or law prohibits a type of telemedicine practice, a violation of that rule can be used in a lawsuit to establish that malpractice occurred. In addition, malpractice insurance policies typically exclude coverage for professional services rendered outside a physician's license.

Consult with a state disciplinary association, an insurance carrier or broker for added insight. It can also be helpful to retain a lawyer who has expertise on malpractice litigation and disciplinary actions to navigate the often complex laws and statutes. Any expenses associated with these steps may be worthwhile if they prevent issues before they occur.

As always, thoroughly document all consultations. A case can be better defended when any potential issues are recognized, analyzed and decided upon with the best information possible.

As telemedicine gains a stronger foothold, some of the issues will begin to resolve. Until then, practitioners must rely on these various resources for guidance.

Linda J. Hay is a member of Hay & Oldenburg, L.L.C., a law firm that is certified as a Women's Business Enterprise, located in Chicago, Illinois. Ms. Hay focuses her practice on the defense of professional liability cases, including medical malpractice. In addition to trial work, Ms. Hay frequently lectures and regularly publishes on risk management issues for professionals. Ms. Hay can be contacted at lhay@illinois-law.com.

Susan A. Wagener is an Associate Attorney at Hay & Oldenburg, L.L.C., a law firm that is certified as a Women's Business Enterprise, located in Chicago, Illinois. Ms. Wagener focuses her practice on the defense of professional liability cases. In addition, Ms. Wagener has lectured on risk management issues for professionals. Ms. Wagener can be contacted at swagener@illinois-law.com.



By Carrie Sherman

The “Do’s and Don’ts” of Telemedicine

For as long as medicine has been practiced, doctors have relied on face-to-face visits to treat patients. But times are changing.

Today, some doctors rely on telemedicine to deliver quality care. It's integral to many major hospital systems and small private practices alike. Nationally, the use of remote healthcare technology to deliver clinical services is significant and growing rapidly—for good reason. When practiced well, telemedicine increases convenience and access while it decreases costs for patients and providers. Studies indicate consistent—and in some specialties, improved—quality and patient satisfaction.

But telemedicine is not without risk. So, whether you've implemented it in your practice or are still in the planning phases, ensure the best possible outcome for you and your patients by considering the following information.

How Will Your Practice Use Telemedicine?

Telemedicine can be used for clinical purposes, as well as for education. Clinically, it is most frequently used to deliver acute primary care. It's also used to deliver care to regions without access to specialists.

Care is delivered through technology in terms of connectivity and equipment. Some practices deliver care interactively in a live format through an “e-visit” with provider and patient using a webcam. Other telemedicine uses include “store and forward.” Patient information is collected at one location then forwarded to another for evaluation and interpretation.

HIPAA Violations Continue to Rise—Experts Agree Many Breaches Still Go Unreported

Since 2009, nearly 30 million Americans have had their personal health information (PHI) breached. There were 199 incidents reported to Department of Health and Human Services in 2013, which translates to 7 million patient records. That's a 138 percent increase over 2012, according to Redspin, an IT security firm.

It's been reported that a senior director of privacy and security for HIMSS indicated that somewhere between 40 million and 45 million patient records have been compromised. So what does this mean for you? Securing PHI must be a priority.

Practices wishing to implement telemedicine should begin by defining the services that are needed. Once this is decided, practices should choose a model of care delivery that best fits the need of the practice. As you develop a business case for telemedicine in your practice, consider these “do’s and don’ts.”

Technology and Security

- **DO choose vendors well.**

In choosing the right technology for your practice, it’s important to work with vendors who understand your practice’s needs. This includes ensuring that equipment supports the practice’s diagnostic needs during clinical encounters. It may also include an understanding of the environmental elements of care that are necessary for the safe use of telehealth equipment. Work with vendors to ensure system redundancy and have in place protocols for equipment and system maintenance.



- **DON’T assume e-visits won’t get interrupted.**

Technology is great, until a storm knocks out the power or your Internet service provider experiences an outage or there are other hardware malfunctions. It’s important for practices to consider how such outages will be handled. If a consult is interrupted, how will connectivity be restored? Also consider how appointments will be continued and whether the data has been captured.

- **DO make security a priority.**

Safeguarding patient data is a major concern for any practice. You should already have in place mechanisms related to HIPAA and Protected Health Information (PHI).

Telemedicine represents new opportunities for data leaks that need to be considered. Providers also need to understand the terms and agreements of each technology service/provider in use. Will the practice need to enter into a business associate agreement with a telemedicine vendor per the terms of HIPAA? Is the vendor meeting the practice’s requirements regarding PHI? The U.S. Department of Health and Human Services provides guidance on business associate agreements, including sample forms, at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

- **DON’T assume your patient also prioritizes security.**

Providers can go to great lengths to ensure their own systems and devices are protected from data breaches, but what about your patients? Patients wishing to engage in telemedicine should understand that their own systems need to be monitored and protected from data breaches. Practices engaging in telemedicine programs that require patients to use their own personal devices for connectivity may need to consider educating patients on basic data monitoring and security protocols. The Federal Trade Commission provides consumer guidance for protecting data online at www.consumer.ftc.gov/.

- **DO develop systems to ensure authenticity.**

Consider protocols for access security (i.e., is the provider who she says she is? Is the patient who he says he is?). Developing policies and procedures surrounding patient

Business Models and Success Strategies

The American Telemedicine Association provides guidance on developing a business case for telemedicine. Learn more at <http://bit.ly/1cgQP7z>.

authentication during an e-visit is critical to any practice’s security measures.

- **DON’T forget about privacy for staff and patient family members.**

Practices should consider how privacy will be ensured for anyone who might inadvertently become part of an e-visit—even a patient’s family member walking past the camera could be an issue. The following provides sample consent forms: www.telehealthresourcecenter.org/toolbox-module/legal-issues-privacy-and-contracting-services.

Compliance & Credentialing

- **DO understand compliance and credentialing related to telemedicine.**

Providers must understand and follow all state requirements and regulations for telemedicine practice, as well as their malpractice insurance requirements. This includes being in compliance with relevant legislation as well as accreditation requirements. And, while telemedicine might make it easy to see patients across state lines, providers must ensure they are appropriately licensed to provide care where their patients are relocated.

Additionally, providers of telemedicine must be credentialed at each individual location where telehealth services are being provided. It’s important for providers to understand the Joint Commission’s requirements for credentialing and privileging.^{1,2}

- **DON'T assume the regulations will stay static.**

Telemedicine legislation—covering everything from licensure to governing bodies to health plan coverage—is being introduced around the U.S. as we speak. Stay up-to-date with what's happening in your state to remain in compliance. The American Telemedicine Association provides up-to-date information about telemedicine legislation at www.americantelemed.org.

Consent & Documentation

- **DO obtain informed consent.**

Ensure your patients are aware of and consent to the potential risks and benefits associated with telemedicine. This could include the potential for delays that result from equipment failure and the potential for security breaches. Talk with your patients about what they can expect from a telemedicine encounter, including those situations when a face-to-face visit is prudent.

- **DON'T forget to document.**

Ensure you've established policies and procedures for documenting e-visits. Documentation allows for continuity of care for the patient. It allows other providers to see what's been done and provides a mechanism for understanding the care delivered should anything go wrong. As always, document any informed consent discussions as well as signed consent forms.

High-Risk Areas

- **DO understand the high-risk areas in your practice and/or specialty.**

The risks that apply to a traditional practice setting also apply to telemedicine. Communication breakdowns and improper handoffs remain an area of risk for most physicians. Other high-risk areas

include errors (medication and diagnostic) and care management issues, like failure to recognize treatment complications. So how does this relate to telemedicine? First, quality of care needs to remain on every provider's radar. In a setting where providers are not able to rely on a physical exam and non-verbal clues, it's important providers delivering care via telemedicine understand how to obtain objective patient information. It's also important to have the clinical context for telemedicine encounters defined.

Providers need to understand the conditions that are appropriate for e-visits and understand which circumstances require an escalation in care. For example, a provider should not use telemedicine in the primary management of chest pain or high fever; however, telemedicine may be an appropriate mechanism for providing advice to a bedside physician caring for said chest pain or high fever.

- **DON'T forget to educate your patients.**

Users of telemedicine services need to understand how to effectively operate the technology that's required. Patients should also understand their legal rights to privacy, as well as how to protect their identities online. Providers need to manage patient expectations for telemedicine, including its limitations. This includes discussions about what and when to report, response times, and provider availability. Technology may be available 24/7, but patients should not expect this from their providers.

Eight Tips to Make the Most of an E-Visit

1. **Connect.** Verbally, express your desire to connect with your on-screen patient. Non-verbally, express this desire by maintaining eye contact, smiling,



nodding—whatever feels comfortable to you. Be sure to adjust the camera height to ensure appropriate eye contact.

2. **Engage.** The e-visit requires reciprocity in order to be successful. Encourage your patient to participate by demonstrating your own interest in the interaction. Again use what feels natural and authentic. Use humor appropriately.
3. **Structure.** Just like your in-person interactions, your online encounters should be organized for effectiveness.
4. **Clarify.** Watch your patient's non-verbal cues for signs you need to further explain. Don't just repeat yourself—use clear language and restate to ensure better understanding. Avoid acronyms, jargon, idioms, and words that can have multiple meanings.
5. **Reinforce.** What does your patient need to know from this interaction? Listeners can't retain everything from a conversation, which is why using techniques like storytelling and repetition can be good tools to help with retention.
6. **Explain.** If you break eye contact with the patient, explain what you're doing. Face-to-face, he could see you're taking notes. On screen it's not obvious and can be perceived as inattention.

Continued from Page 5



7. **Synthesize.** Ask your patient to repeat what she's learned and what you expect her to do next. It's your job to ensure your communication was effective.
8. **Reimbursement.** Reimbursement of telemedicine charges should be clarified up front.

Checklist for Training and Development

Training

- Staff and patients have been provided guidance around enhancing communication skills, including video presentations.
- Staff and patients understand the scope of services to be provided and when a patient needs to be seen physically.
- Staff is familiar with the system and practice protocols surrounding telemedicine.

- Operational protocols associated with telemedicine have been established and include how deviations from regular practice protocols should be handled.
- Staff understands how to respond to equipment malfunctions.
- Staff is trained to recognize unhappy, uncooperative patients and understand their roles in identifying such patients.

Consent and Documentation

- Patients and staff understand the risks that are inherent in telemedicine (e.g., incomplete or failed transmissions, corrupted files, data breaches, natural disasters, and more).
- Policies and procedures are established that define the maintenance of e-visit records.
- Consent forms provided during e-visits are properly signed and documented.

Technical

- Technology is in place to support necessary diagnostic elements.
- Equipment and system maintenance is appropriately considered.
- Critical connectivity is ensured through appropriate redundant systems.
- Appropriate redundant clinical video and exam equipment for critical clinical encounters is in place.



Scan to visit the
risk management section of
psicinsurance.com

Administration

- Policies and procedures have been implemented to address quality improvement and performance management.
- Providers are compliant with all relevant legislation, regulations, and accreditation.
- Scope of services has been defined and appropriate written agreements and/or contracts are in place.

Carie Sherman is a freelance writer based in Denver, Colorado. She has more than a decade of experience in the professional liability industry and works with a variety of healthcare clients, including the Colorado Hospital Association and the University of Colorado, School of Medicine. Carie Sherman has been published by various publications, including Colorado Parent.

1. www.jointcommission.org/assets/1/6/Pre_Pub_Telemedicine_HAP.pdf
2. www.jointcommission.org/assets/1/6/Revisions_telemedicine_standards.pdf

Legal Defense Coverage for State Disciplinary Proceedings

PSIC's policy provides coverage of up to \$25,000 in legal expenses to represent its physician insureds at state disciplinary proceedings. If you receive notice of a licensing board inquiry or investigation (or think one may be forthcoming), contact our claims staff at 1-800-640-6504. They will discuss the issues with you, offer advice, confirm your specific available coverage and take action where appropriate.



Send all inquiries, address changes and correspondence to:
Physician Connection, P.O. Box 9118, Des Moines, IA 50306
Toll-Free 1-888-336-2642
Internet – www.psicinsurance.com
Email – riskmanagement@psicinsurance.com

Physician Connection is published for policyholders of Professional Solutions Insurance Company. Articles may not be reprinted, in part or in whole, without the prior, express consent of Professional Solutions Insurance Company.

Information provided in *Physician Connection* is offered solely for general information and educational purposes. All names used in *Physician Connection* are fictional. Any relationship to actual people is purely unintentional. It is not offered as, nor does it represent, legal advice. Neither does *Physician Connection* constitute a guideline, practice parameter or standard of care. You should not act or rely upon this information without seeking the advice of an attorney.