the REPORTER

CME: THE INCREASED USE – AND RISKS – OF SOCIAL MEDIA IN A HEALTH CARE SETTING

USING AI MEDICAL SCRIBES: RISK MANAGEMENT CONSIDERATIONS

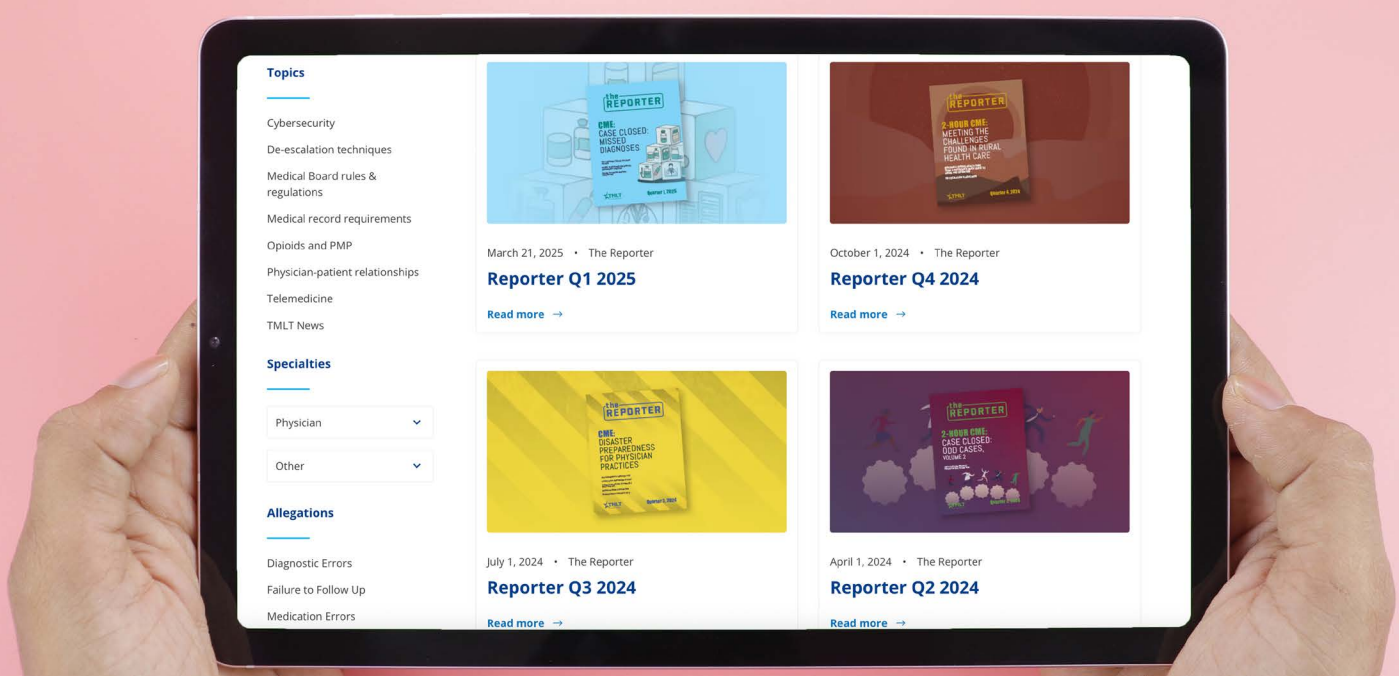
CLOSED CLAIM STUDY: FAILURE TO PROPERLY MANAGE PATIENT'S CENTRAL VENOUS CATHETER

CLOSED CLAIM STUDY: DELAY AND FAILURE TO DIAGNOSE CHOLESTEATOMA

TMLT
Texas Medical Liability Trust

Quarter 2, 2025

Read or download back issues of *the Reporter*, from 1998 to today.



www.tmlt.org/reporter

Letter from the editor:
the Reporter: A new beginning

Dear readers,

This is the last print issue of *the Reporter.*

Keep an eye on your email inbox for the next issue, an all-new digital version, coming to you in August.

For more than 30 years, it has been our privilege to deliver *the Reporter* to your homes and offices. In that time, we've offered stories, industry news, and information that matter—to you, your colleagues, and your patients. Today, I'm writing to announce an exciting development in our publication's evolution.

This year, *the Reporter* will become exclusively digital—available anytime, anywhere—on our website, www.tmlt.org. With the new digital *Reporter,* you will enjoy access to breaking stories; searchable archives of past issues; and the valued features that you've come to expect from *the Reporter*, such as CME articles and TMLT case studies.

Our first all-digital edition of *the Reporter* will be our next issue, the Quarter 3 edition for 2025, launching this fall.

Thank you for being a part of TMLT. We look forward to experiencing this new beginning for *the Reporter* with you.

Sincerely,

Wayne Wenske
Editor, the Reporter
Texas Medical Liability Trust (TMLT)
wayne-wenske@tmlt.org

CONTINUING
MEDICAL
EDUCATION

CME:
THE INCREASED USE – AND RISKS – OF SOCIAL MEDIA IN A HEALTH CARE SETTING

by Roxanna Maiberger, JD, MPAff

The closed claim study in this article is based on an actual malpractice claim from Texas Medical Liability Trust. This case illustrates how action or inaction on the part of the physicians led to allegations of professional liability, and how risk management techniques may have either prevented the outcome or increased the physician's defensibility. This study has been modified to protect the privacy of the physicians and the patient.

OBJECTIVES

Upon completion of this educational activity, the learner should be able to:

1. identify and remediate the pitfalls for a medical practice using social media;
2. describe HIPAA-compliant communication methods for online physician-patient interactions;
3. discuss how COVID-19 has affected the physician-patient relationship via increased use of online communications; and
4. apply risk management strategies when interacting with the public online.

COURSE AUTHOR

Roxanna Maiberger is a civil litigation attorney with Mayer LLP. She earned her undergraduate and graduate degrees from The University of Texas at Austin. She earned her law degree from St. Mary's University School of Law in San Antonio. Before attending law school, she worked for Texas Medical Liability Trust as a risk management representative.

DISCLOSURE

Roxanna Maiberger has no relevant financial relationship(s) with ineligible companies to disclose. TMLT staff, planners, and reviewers have no relevant financial relationship(s) with ineligible companies to disclose.

TARGET AUDIENCE

This 1-hour activity is intended for physicians of all specialties who are interested in learning more about risks associated with communicating online with patients via social media and developing risk management skills to avoid potential liability when interacting with these platforms.

CME CREDIT STATEMENT

The Texas Medical Liability Trust is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

The Texas Medical Liability Trust designates this enduring material for a maximum of 1 *AMA PRA Category 1 Credit(s)™*. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

ETHICS CREDIT STATEMENT

This course has been designated by TMLT for 1 credit in medical ethics and/or professional responsibility.

TEST

To receive CME credit, physicians should complete the test questions that follow the activity. A passing score of 70% or better earns the physician 1 CME credit.

PRICING

The following fee will be charged when accessing this CME course online at http://tmlt.inreachce.com.

Policyholders: $10
Non-policyholders: $75

INSTRUCTIONS

CME test and evaluation forms must be completed online. After reading the article, go to http://tmlt.inreachce.com. Log in using your myPortal account information to take the course. Follow the online instructions to complete the forms and download your certificate. To create a myPortal account, go to www.tmlt.org, click the log in button, and follow the on-screen instructions.

RELEASE/REVIEW DATE

This activity is released on June 10, 2025 and will expire on June 10, 2028. Please note that this CME activity does not meet TMLT's discount criteria. Physicians completing this CME activity will not receive a premium discount.

INTRODUCTION: DEFINING SOCIAL MEDIA

There is no question that social media is here to stay. Yet, questions persist around how intertwined social media should be in our daily — and professional — lives. Social media is often defined through its most popular and ubiquitous platforms: Facebook, LinkedIn, Instagram, and TikTok, with more social media platforms seeming to pop up every day.

But "social media" encompasses more than the traditional platforms used by everyday consumers. Merriam-Webster defines social media broadly as "forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)."[1]

This basic definition shows how expansive and potentially wide-ranging social media is, even extending to the inclusion of online reviews or applications for capturing user data.[2] This broad definition surely encourages positive outcomes through information sharing, but social media is not without its own set of risks.

Although outside the scope of this article, an important consideration in terms of social media's increasing presence, is its intersection with "Big Data." Big Data refers to large databases and the process of analyzing the information stored within these databases.[2] The information captured includes personal data harvested from use of electronic applications, such as fitness tracking applications or retail purchase receipts.

In terms of health care, Big Data may consist of electronic health record (EHR) data and medical research data. When considering the intersection between physician-patient interactions within such applications as EHR interfaces and online patient reviews, the potential of Big Data exposures triggers HIPAA concerns and highlights the risks associated with the use of social media.

This article focuses on health care professionals' use of social media for professional purposes and does not center on personal use of social media. However, when interacting with social media for personal use, especially if one's platforms are available for public view, it is important to be aware of the associated safety and medical liability risks.[3]

Unfortunately, we live in a world where patient dissatisfaction can escalate and become a threat to personal safety. So, it is good risk management practice to adopt the same or similar boundaries that you would use for in-person interactions when interacting online. It is important to approach social media use in terms of a security assessment from a virtual and physical risk assessment standpoint.

For example, some social media platforms allow you to disable commenting on posts, which can curb unwarranted and unnecessary patient comments. If comments or posts by patients are allowed on the social media platform, consider assessing the settings that allow individuals to comment or interact with a health care practice social media page. Further, assess your own personal social media security and privacy settings to ensure you are not leaving yourself open to unwanted negative interaction.

This article emphasizes that the increasing presence of social media and technology is the "new normal" and needs to be faced and managed. This new normal also presents an opportunity for health care professionals to proactively consider all internet-based communication and information sharing when embarking on patient care and managing a health care practice.

Ultimately, the goal of this article is to provide risk management considerations for health care professionals when facing the increasingly complex realm of social media. This article will discuss the following:

- the intersection of social media with the physician-patient relationship;
- the pitfalls of and the risk management considerations for social media and the physician-patient relationship, including ethical dilemmas, informed decision making, and when to call your professional liability insurer or seek legal advice;
- HIPAA concerns associated with the risks of social media;
- the ongoing impact of COVID-19 and the increased use of telemedicine and social media; and

- future considerations for social media use and the virtual reality for physicians.

This article will also help you plan ahead and address unanticipated social media and patient interaction concerns. Specifically, we will explore guidelines for creating general policies and procedures on social media for physicians and their staff members.

The information in this article should not be used or referred to as a primary legal source. Instead, it is a best practice to consult with your attorney to create policies and procedures that ensures your practice complies with your state's health care laws and medical board rules.

SOCIAL MEDIA MEETS THE PHYSICIAN-PATIENT RELATIONSHIP

Social media maintains an ongoing, permanent presence in health care because we live in an "online world." Specifically, social media intersects health care in:

- physician practice advertisements and promotions;
- communications through EHR systems; and
- the ability of patients to leave their thoughts and/or comments online for public consumption.[4]

Patients have the right to express their positive feelings or frustrations following an experience with a health care provider or practice. The danger is that these (one-sided) posts often describe events out of context or bypass the nuances of the interaction (i.e. body language, tone of voice, patient history unknown to the public) or of the physician-patient relationship (a long history of patient noncompliance or one of deep trust).

There are certainly positive aspects of social media use in health care, such as patient education and increased communication between patients and their respective health care teams. However, the negative experiences of social media often remain top of mind because of the headaches they can cause.

One negative outcome of social media is that it can contribute significantly to stress and burnout for physicians and other health care professionals.[5] It is undeniable that health care rules and regulations set in motion by the increased presence of social media can seem impossible to comply with, especially for smaller health care practices already stretched thin.[4]

However, the good news is that with the proper tools and information, many of these social media concerns can be planned for appropriately.[4] Taking the time to think through possible scenarios can lessen the stress caused when a negative interaction between patients and health care professionals occurs. Just as negative interactions may occur with patients in-person, the same is true for interactions with patients online.[6]

PITFALLS AND AREAS OF CONCERN

Although the definition for social media technically could include patient and health care professional interactions and/or communications within a practice's respective EHR system, the main focus of these interactions center on the pitfalls stemming from public-facing social media channels. This typically manifests itself in the form of a patient leaving a negative comment or feedback in an online review.[6]

As previously discussed, social media is an important tool for health care professionals as they progress through their careers. Notably, the use of social media to promote health care practices cuts both ways, because an overwhelming majority of patients likely consult online reviews before choosing a physician and/or heath care professional to meet.[6] As a result, a negative review may carry significant weight to a health care professional's reputation, especially for residents and physicians beginning their careers. This creates a vulnerable situation for physicians because it, understandably, places them in the defensive position of protecting and maintaining their reputations.[6]

However, it is important to point out that one bad review, while possibly a temporary setback, is unlikely to tarnish one's medical career long term. Perspective is key here. Most people look at the totality of online reviews when choosing a health care professional and may even take a few negative comments with a grain of salt.[7]

Many patients don't look at online reviews or comments at all. A recent study from the *Journal*

of Patient Experience shows that patients give more credence to recommendations from family or friends (55 percent "important" vs. 36 percent "not important") than to online reviews (43 percent "important" vs. 47 percent "not important") when seeking a physician.[8]

Also, it is important to consider that according to research, 50 percent of negative online reviews left by patients stem from "poor communication."[6] Poor communication is introduced in quotes because this complaint can be hard to define and could cover a host of scenarios. "Poor communication" is a subjective phrase, and will undoubtedly mean something different to each patient. Another subjective reason could be "poor staff interactions." This could refer to anything from not getting a preferred appointment time to perceived rudeness from a receptionist.

When coming across negative online reviews for you or your practice, it is important to first pause and to not respond.[6] Treat it as you would treat an email from an angry or frustrated patient. Walk away and give yourself time to think about a warranted response, if any. Consider the following in managing a negative online review.

Though it is frustrating for physicians, patients are entitled to share their feedback online.[6] Accepting this reality opens the opportunity for health care professionals to focus on handling and mitigating the impacts of a negative review as opposed to being stuck on whether it's fundamentally fair or not.

An equally important consideration is to be honest and assess whether there is any truth or validity to the patient's comments. Although this may be uncomfortable, thinking this through can serve as a critical strategy in mitigating the aftermath of a negative online patient review.[7]

Assessing the validity of a patient's comments may lead to a re-evaluation of systems in place for a health care practice. Rather than allowing the patient's negative comment to serve as an indicator of being right or wrong, let it serve as a check and balance to the overall functioning of practice systems. It

could create an opportunity for change, even if it is uncomfortable in the moment.

When deciding how to respond to an online comment or post, the most critical consideration is to maintain patient privacy and HIPAA compliance. (Because of HIPAA's importance and complexity, it is discussed at length in the next section.) ***The best practice is to avoid responding.*** However, consider the possibility of seeking clarity from the patient *through private (offline) one-on-one communication.*

If the patient is identifiable, seeking an individualized, non-public, one-on-one interaction with the frustrated patient will likely de-escalate the situation. Even if the patient is frustrated, they will likely remember a physician, health care provider, or a member of the health care team who picked up the phone and tried to understand their frustration and find a solution to prevent it in the future *to the extent it is feasible.* This action removes most concerns of the Health Insurance and Portability and Accountability Act (HIPAA) about direct responses to a patient's online comments.

Should a health care professional choose to reach out to a patient, avoid making excuses or blaming the patient. Instead, take ownership of the situation that created the patient's frustration. From a risk management perspective, this can allow the patient to feel heard, understood, and validated. Listening to understand as opposed to listening to be right about the situation will likely lead to a more productive dialogue. **It is also inappropriate to ask a patient to remove their negative online comment.**[6]

If the patient's comment alludes to an ongoing medical emergency, it may become necessary to call the patient and direct them to emergency health services or to call 911. Document these efforts accordingly.

HIPAA AND SOCIAL MEDIA

Significant privacy protections for patients were added after passage of HIPAA.[9] The act was also passed partly in response to technology advancement and the potential "erosion" of health information privacy.[9] Although well intended, the application of HIPAA's privacy rule undoubtedly complicates day-to-day activities for physicians and staff. For example, even corresponding with another member of the health care team about a patient's care is under the microscope to ensure the interactions were "HIPAA compliant."

Even then, assessing whether a communication platform is truly "HIPAA compliant" raises questions outside the scope of this article. When issues arise related to HIPAA and the use of protected health information (PHI), reach out to your medical professional liability insurer, your state's medical association, and/or your health care attorney for guidance.

Because HIPAA consists of federal rules and regulations, state law may vary from the HIPAA rules and regulations. In some instances, state laws governing patient privacy and data may have even more stringent requirements.

In the event a health care professional chooses to respond publicly to a patient's online comment, *whether it be a negative or positive comment,* each response should use a general, uniform statement as a means of ensuring HIPAA compliance. For instance, general statements could be:

- "Thank you for your comment. We value feedback. Due to patient privacy regulations, we cannot discuss details mentioned in your comment. If you are a patient, please contact our office at [insert your office's contact information] to discuss this further should you have additional comments or suggestions."
- "In order to protect our patients' privacy, all patient concerns and complaints are resolved directly by our practice and not through social media. If you are a patient, please contact us at [office contact information]. Thank you."
- "Thank you for your comment. At our medical practice, we strive to provide the highest levels of patient satisfaction. Due to federal privacy laws, it is not the policy of [insert practice name] to substantively respond to negative reviews on ratings websites. If you are a patient and have a concern, please contact us at [phone number]."[10]

These uniform responses can help you plan ahead if and when a patient leaves a negative comment on a social media page. When planning these uniform responses, the response from a health care professional should always be respectful. It is also good practice to thank them for their feedback.

Additionally, if you are ever unsure whether a comment complies with HIPAA, it is best to consult your health care attorney.

The response *should never* allude to or state that the patient received care from the physician, health care professional, or practice, as this reveals PHI. Lastly, the comment should include contact information so the patient can speak with the health care practice directly. This effectively provides the patient a way to voice their complaints without expressly identifying them as a patient of the health care practice.[7]

Remember that HIPAA is *not* a two-way street. While a patient can state publicly that they are a patient of the physician or health care practice, the physician or health care practice cannot do the same in return. Doing so is a HIPAA violation.[7] Further, health care practices are required to provide HIPAA training to all staff.

Consider these general guidelines when responding to a patient's online comment.

- When in doubt, do not respond.
- Consider whether a general online response is even warranted — specifically, consider whether a response may be better received by the patient offline.
- If you feel strongly that you must respond online, keep any response general and non-specific. Provide information for the patient to call the office if they so choose.
- Never disclose any of the patient's information or acknowledge that they are a patient of your practice.

In the event of an alleged HIPAA violation, it is important to immediately contact your medical professional liability insurer, as they may have resources to help you navigate the reporting requirements and associated bureaucracy.

Moreover, because state laws vary, keep in mind that HIPAA violations may have different implications in the event of a lawsuit by a patient affected by the wrongful disclosures of information. Certain state laws may even vary by certain medical conditions. In addition to varying rules by state, within each state, certain courts may vary in their interpretation of the rules. This highlights the importance of consulting an attorney who is well-versed in HIPAA compliance and state-based patient privacy laws.[11]

The complexity of HIPAA and state-based patient privacy laws supports the recommendation to proactively and consistently train health care staff and consider the supervisory protocols for the practice. In addition, privacy and security protocols are required by federal law. These protocols should be clear and understandable. It is more than simply drafting protocols once and never reviewing them again. At a minimum, the protocols should be reviewed annually and updated in accordance with the health care practice's growth and changes over time.

Additionally, working with your EHR and/or IT vendors to better understand how your patients' data is being used could be beneficial and provide an increased sense of control over your practice's electronic resources and assets. It may be beneficial to speak with your medical professional liability insurer to understand its expectations and steps to take in the event of a data breach. Certain notification timelines may apply to ensure you are covered or qualify for assistance in remedying the breach.

Examples of data breaches for PHI in the context of social media could be:

- responding to an online review with specific information that identifies the writer as a patient;
- posting photos to a practice website without the patient's consent that includes potentially identifying information, such as a patient's face, tattoos, or other unique physical identifier. If a patient consents to posting of photos on a website or social media, written consent should be obtained after review by the patient of each specific photo to be posted;
- posting photos to a practice website in which the metadata[12] has not been properly removed, resulting in the file name identifying the patient's information when hovering a cursor over the image; and
- improperly disposing of PHI (i.e. throwing papers with PHI in a trash can without properly shredding the documents).[13]

The following case study illustrates how a patient's PHI was breached online.

CASE STUDY — PATIENT IDENTIFIED ON SURGEON'S WEBSITE

A plastic surgeon's website featured "before and after" photos of patients. The patients' consent to post photographs was obtained, names were not used and the photos were posted in a way that preserved patient anonymity.

However, unknown to the plastic surgeon and his staff, the patients' names had not been properly removed from the meta tags associated with the photos. Meta tags are content descriptors that describe web page content to search engines. Meta tags do not appear on the page, but are found in the HTML code for the page.

The issue was discovered when a patient performed a Google search on herself and her images from the plastic surgeon's site appeared in the search results. Although he was told about the meta tag issue, the plastic surgeon did not immediately remove the photos.

Fifteen patients filed lawsuits against the plastic surgeon. The Office of Civil Rights also investigated the plastic surgeon for possible HIPAA violations.

Risk management considerations

- Obtain written patient consent to take photographs. Specify how you plan to use the photos (i.e. medical records only, marketing, website, journal article) on the consent form. Have the patient review and approve the specific photos to be posted prior to signing the consent form.
- Do not name or save photo files with any of the identifiable information (described previously) in any publicly accessible area. (Clearly, if you are just adding photos to medical records, they can contain identification.)
- Audit photos that have been added to your website. Check the site page for tags, meta tags, alt text, keywords, or anything that could be used to identify patients.
- Do not store photos of patients in an unencrypted device, such as a camera, cell phone, tablet, or personal laptop.

When it comes to publishing patient photos, certain HIPAA requirements must be met. If patient photos are completely de-identified, HIPAA requirements are satisfied. If patient photos are not de-identified, written authorization from the patient is required to

post or share the photos. From a risk management standpoint, specific written authorization/consent is recommended for any posting of patient photographs.

THE INCREASED ONLINE PRESENCE FOR PHYSICIANS IN A POST-COVID WORLD

The COVID-19 pandemic fundamentally changed how people communicate because it required an increase in the use of virtual technology and the need for remote work. For physicians, COVID-19 solidified the increased need and use of telemedicine almost overnight. This led to the need to build an online presence, including social media.[14]

From HIPAA compliance and risk management perspectives, telemedicine further complicates patient privacy concerns.

The presence of virtual health visits and the general population's reliance on telehealth technology persists. The "option" to communicate through online platforms or social media remains an acceptable alternative form of communication for many. This increases the need for physicians to be aware of the implications and pitfalls of online interactions to promote and advertise health care practices; using social media for health care educational means; and more.

In sum, increased presence means increased risk.

To be better prepared for this increased risk, it is important to accept the reality that technology will continue to progress faster than regulations and legislation will keep up.[2]

Effective planning requires anticipation of the risks and pitfalls of social media use discussed previously and promotes intentional and informed decision making. This planning can include the following items.

- Use state-based resources. For example, the Texas Medical Association (TMA) provides a wide array of resources from sample policies to useful articles to help you prepare your practice for HIPAA compliance and protect PHI. Consult your state medical association to inquire about the resources available to you.
- Consult with your health care liability insurer, as it may provide HIPAA consultation services or risk management resources.
- Remember that there is no need to reinvent the wheel when it comes to creating policies and procedures. There are numerous resources available with pre-templated policies. **However, it is important to take the extra step of customizing these templates to suit the needs of your individual practice.** Simply purchasing templated policies and keeping an electronic copy in your drive or placing them on your office shelf is not sufficient. It is critical you develop your policies into identifiable and verifiable action.
- Provide your patients with information on these topics. This may start with your patient intake forms and ensuring you have the proper Notice of Privacy Practices and other required information when it comes to PHI. Educating patients from the outset not only protects you, but it also sets expectations with your patients about the physician-patient relationship. Additionally, sharing this information encourages further communication with your patients and may prevent them from feeling unheard and without a sense of recourse — potentially eliminating a motive for negative online comments.
- Most importantly, remember that most situations can be resolved with intentional and thoughtful offline communication.

PERSONAL SOCIAL MEDIA USE

When it comes to personal social media use, it is important for physicians to remember that their online presence will never be completely personal or private. Patients, patients' family members, or others in the community may conduct online searches to find out more about you, your role at work, or your friends and family.

When posting on social media platforms using your personal account, never disclose trade secrets, intellectual property, or other confidential information about your practice, organization, or yourself. If you comment online in support of your organization, including its products or services, be sure to clearly disclose your relationship with the organization.[15]

It is also important to consider not accepting "friend requests" on social media platforms from patients. If you do, you risk losing appropriate professional boundaries with patients. Also, if your professional relationship becomes unwittingly disclosed on social media, your patient's privacy may be compromised, and you could be in violation of HIPAA. Although some shared banter on mutual interests can help build rapport between physicians and patients, excessive self-disclosure is unlikely to help in the clinical setting. Such disclosures could lead to boundary violations, legal, sexual, or otherwise.[16] The big takeaway is that the use of social media to communicate with patients can be a slippery slope.

In addition, make it a practice not to accept friend requests from anyone that you do not know personally, including friends of friends. When a friend request is accepted — unless privacy settings are specifically adjusted to restrict access — that person can view all your personal information, familiarizing themselves with your nearest friends, family members, and associates.[15] From a risk management perspective, consider reviewing your privacy and security settings regularly to ensure the settings are appropriate.

CONCLUSION

Social media is here to stay — as is its intersection with health care practices and health care professionals. Although there are several positive aspects of social media in health care, there are also some potential pitfalls.

These pitfalls primarily involve ensuring HIPAA compliance; state-based patient privacy laws; and wrongful disclosure of PHI. As a way to avoid these pitfalls, be proactive and plan for these scenarios.

Effective planning consists of consulting state-based medical association resources, your medical professional liability insurer, and/or your health care attorney. Most importantly, personal communications with patients offline may be the best way to resolve patient complaints, prevent future ones, and protect against HIPAA compliance issues.

SOURCES AND NOTES

1. Social Media, Merriam Webster Dictionary online. Available at https://www.merriam-webster.com/dictionary/social%20media. Accessed May 2, 2025.
2. Parker DM, Pine SG, Ernst ZW. Privacy and Informed Consent for Research in the Age of Big Data. Penn State Law Review. Volume 123, Article 4. Spring 2019. Available at https://elibrary.law.psu.edu/pslr/vol123/iss3/4/. Accessed May 2, 2025.
3. Chipidza F, Wallwork RS, Adams TN, Stern TA. Evaluation and Treatment of the Angry Patient. Primary Care Companion for CNS Disorders. June 2016. Available at https://pmc.ncbi.nlm.nih.gov/articles/PMC5035812/. Accessed May 2, 2025.
4. Gosfield AG, Shay DF. The physician's electronic reality. Health Law Practice Guide § 38:9. March 2025 update. American Health Lawyers Association.
5. Singh R, Volner K, Marlowe D. Provider Burnout. Updated June 12, 2023. StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing. S025. Available at https://www.ncbi.nlm.nih.gov/books/NBK538330/. Accessed May 2, 2025.
6. Physician's Weekly. How physicians can safely respond to negative online reviews. June 21, 2024. Available at https://www.physiciansweekly.com/how-physicians-can-safely-respond-to-negative-online-reviews/. Accessed May 2, 2025.
7. American Medical Association. Are physicians prohibited from responding to online patient reviews? April 26, 2022. Available at https://www.ama-assn.org/practice-management/hipaa/are-physicians-prohibited-responding-online-patient-reviews. Accessed May 2, 2025.
8. Kozikowski A, Morton-Rias D, Mauldin S, et. Al. Choosing a Provider: What Factors Matter Most to Consumers and Patients? Journal of Patient Experience. January 19, 2022. Available at https://pmc.ncbi.nlm.nih.gov/articles/PMC8785326/. Accessed May 14, 2025.

9. Tucci E. #NoFilter: A critical look at physicians sharing patient information on social media. Indiana Health Law Review. Volume 16. No 2. 2019. Available at https://journals.indianapolis.iu.edu/index.php/ihlr/article/view/23322/22619. Accessed on May 2, 2025.
10. Responding to online patient complaints. Texas Medical Liability Trust. Available at https://www.tmlt.org/articles/responding-to-online-patient-complaints-2. Accessed May 14, 2025.
11. Sanson CK. Cause of action against physician or other health care practitioner for wrongful disclosure of confidential patient information. Causes of Action Second Series. March 2025 updated. Clark Boardman Callaghan, publisher.
12. Metadata is information within a data point or data set that reveals information about authors, the creation of the data, or the file size. This can be found in items such as digital photos, documents, and other types of data being shared electronically. IBM. What is metadata? September 2024. Available at https://www.ibm.com/think/topics/metadata. Accessed May 13, 2025.
13. HIPAA Privacy Rule. Department of Health and Human Services. National Institutes of Health. Available at https://privacyruleandresearch.nih.gov/pr_08.asp. Accessed May 2, 2025.
14. Fowler LR. COVID-19 & the myth of health data privacy. Kansas Journal of Law & Public Policy. Summer 2022.
15. Social media and cyber risk management. Texas Medical Liability Trust. Available at https://www.tmlt.org/resource/social-media-and-cyber-risk-management. Accessed May 14, 2025.
16. Chang Chretian K. Should I Be "Friends" with My Patients on Social Networking Web Sites? American Family Physician. July 1, 2011. Available at https://www.aafp.org/pubs/afp/issues/2011/0701/p105.html. Accessed May 14, 2025.

Roxanna Maiberger can be reached at rmaiberger@mayerllp.com

USING AI MEDICAL SCRIBES: RISK MANAGEMENT CONSIDERATIONS

by Wayne Wenske, Senior Marketing Strategist

According to a new study from the American Medical Association (AMA), 66 percent of physicians reported using artificial intelligence (AI) tools or systems at work in 2024, representing a 78 percent increase in use from 2023. Among the most quickly adopted AI applications has been medical scribes — AI systems designed to automatically document patient encounters, generate clinical notes, and assist with medical documentation. These tools promise to ease physician stress and burnout by reducing time spent on administrative tasks, while improving documentation quality.[1]

"These AI assistants can reduce a physician's time devoted to documentation by up to 70 percent by transcribing patient encounters, entering data into EHRs, and processing information for orders and prescriptions, allowing physicians to focus on direct patient care."[2]

However, as AI medical scribes become commonplace in clinical settings, the same AMA study shows that physicians are concerned with the risks AI presents to patient privacy, accuracy of documentation, or other liability risks.

THE BENEFITS OF AI SCRIBES

AI scribes have become popular due to increased documentation demands over the past decade. The AMA found that physicians spend an average of "5.8 hours per eight hours of time scheduled for patients on documentation duties, with a significant amount of that time spent outside of scheduled clinical hours." These demands contribute significantly to professional frustration and burnout.[3]

AI scribes use "machine learning" (a type of AI that allows systems to learn from data without human programming or prompts); "natural language processing" (AI that enables systems to interpret and use human language);[4] and other capabilities to:

- record and summarize patient-physician conversations;
- extract relevant medical information from discussions;
- input data directly into EHR systems; and
- recommend medical codes for billing and compliance purposes.

Physicians can then review, edit, and sign the AI-generated notes in the medical record. This last step is vital to avoid documentation errors, omissions, or misrepresentations of the encounter. Skipping this step could increase medical liability risk.

CAVEATS FOR PHYSICIANS USING AI MEDICAL SCRIBES

1. Documentation inaccuracies and omissions

AI medical scribes are certainly not perfect. These systems, also called "ambient medical scribes," translate recorded interactions and input them into the patient record. These systems may:

- miss critical clinical information discussed with the patient;
- incorrectly transcribe medical terminology;
- omit important non-verbal observations;
- "hallucinate" or create information about a patient simply to provide an answer in an EHR template or fill in an information gap;[5]
- misinterpret vague statements or questions; or
- omit contextual factors that influenced clinical decision-making.

There are also concerns about AI scribes relying on generalized, historical data the system may encounter that perpetuate racial, sexual, age-based, and other biases. When past biases are introduced into the AI system, there is a potential for perpetuating discriminatory practices or less inclusive treatment.[8]

2. Reduced critical review

As physicians and other health care professionals grow more accustomed to using AI-generated documentation, there may be a temptation to spend less time reviewing what has been recorded. This may result in signing off on notes without careful review; not catching mistakes in the patient record; making assumptions that important information was captured; or not applying appropriate critical thought to what was documented.

AI systems, even those with high accuracy rates, can make mistakes, especially in complex cases. This makes physician review imperative. "Uncritical acceptance of AI suggestions carries the risk of errors in the chart."[2]

3. Concerns regarding legal authorship and authentication

When using an AI scribe to generate a physician's

notes, consider the following legal questions.

- Who is legally responsible for the AI-generated content?
- How are physician observations and AI-generated content differentiated?
- How appropriate or "safe" are automatic signatures on AI-generated content?

The Federation of State Medical Boards has issued guidance emphasizing that physicians remain fully responsible for the content of all medical documentation, regardless of how it was generated. Therefore, physicians must take the time and care to ensure AI-generated content and patient records accurately reflect their professional assessment of the patient, care goals, and the treatment provided. Automatic signatures on AI-generated content are discouraged.[6]

4. Privacy breaches and HIPAA concerns

Because AI medical scribe notes are based on audio recordings of patient-physician conversations, there is a built-in potential for breaches of patient privacy. These conversations may include mentions or confirmations of HIPAA-protected patient information, such as patient name, birthdate, address, contact information, family member names and contact information, pre-existing conditions, or other protected health information (PHI). In turn, this information becomes vulnerable in the event of a cyber security breach; inappropriate storage or transmission of PHI; or sharing PHI with third-party AI vendors.

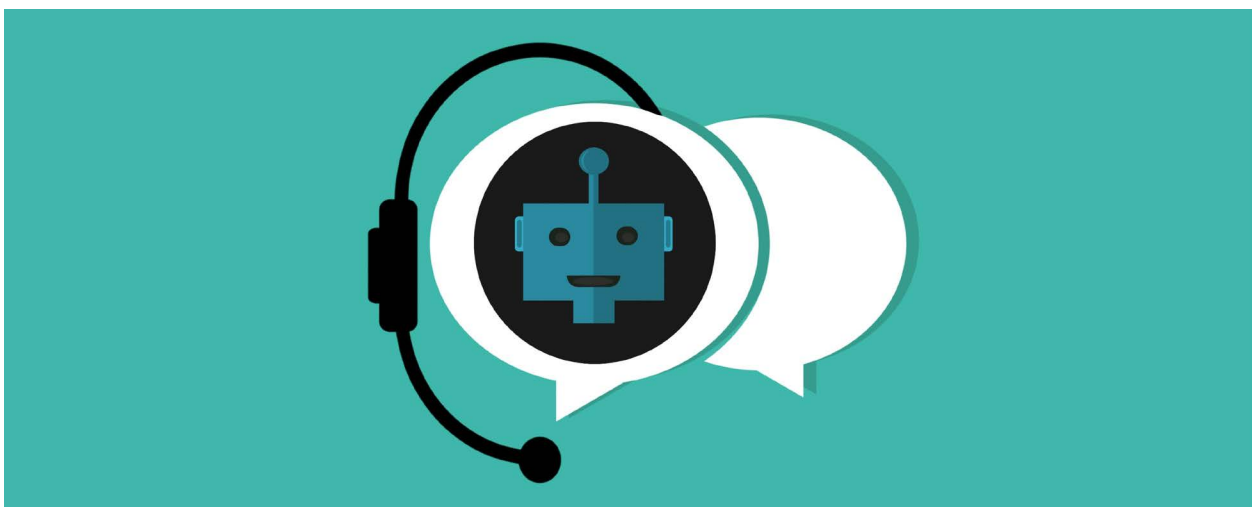
The Office for Civil Rights (OCR) maintains that health care providers covered by HIPAA remain responsible for mitigating or preventing cyber-threats to patient PHI.[7,8] Before choosing an AI scribe software, review their protocols and security measures to ensure HIPAA compliance. In addition, a Business Associates Agreement (BAA) should be executed. If AI scribing is built into your current EMR system, verify with the software vendor that the integrated AI scribing portion is not offered by a separate vendor. If it is managed by a separate vendor, consider obtaining a separate BAA.

5. Informed consent challenges

The use of AI scribes also raises questions about patient consent for the use of AI in their care and treatment.

- Are patients adequately informed that AI is recording and processing their conversation, symptoms, and diagnoses?
- Do patients understand how their PHI will be used and analyzed by the AI system?
- Have patients been given the opportunity to opt out of having an AI scribe or system used in their care?
- If applicable, do your consent forms provide information on how patient data may be used by AI to "train" the system?

Several states now require explicit consent from patients for the recording and processing of health care encounters using AI. Failure to obtain consent could lead to claims alleging violations of patient privacy.[9] Obtaining patient acknowledgment



and consent for the use of AI scribe systems is recommended.

6. Risks of using clinical support features
Some advanced AI scribe systems include clinical support features, such as suggesting diagnoses, recommending tests, or identifying medication interactions. These features carry additional risk for a physician, including:

- relying on AI clinical suggestions without careful review and agreement;
- unclear notes on which recommendations came from AI and which came from the physician; and
- errors in AI clinical suggestions based on limited information or training received by the system about a specific condition, medication, or procedure.

These types of risks may be hard to defend in the event of a claim due to a misdiagnosis or other diagnostic error traced to AI use.

RISK MANAGEMENT STRATEGIES WHEN USING AI SCRIBES

Consider the following steps when using AI medical scribes.[8, 10, 11, 12]

1. Establish strict review protocols

- Amend your current documentation policies and procedures to include review of all AI-generated documentation and content.
- Set aside dedicated time each day to carefully review documentation and make any needed edits prior to sign-off.
- If an error is noted after the AI-generated note has been finalized and signed, correct it via an addendum or amendment, which clearly shows the corrections made, including name of physician or provider reviewing the notes, date of review and error found. Follow applicable state rules regarding documentation.

  For example, the Texas Medical Board rule 163.1 requires "clear identification of any amendment or correction to the medical record, including the date it was amended or corrected and the identity of the author of the amendment or correction, with the original text remaining legible."[13]

2. Include AI scribe use in consent forms and procedures

- Add language to your patient consent forms that addresses AI scribe use. Explain the technology and its purpose in your informed consent discussions with patients using clear, non-technical language.
- Train staff on how to clearly explain AI documentation processes to patients.
- Document all consent discussions in the patient's record.

3. Train staff on AI scribe/documentation use

- Ensure all physicians and staff receive thorough training on the use and risks of AI scribes.
- Regularly update training as AI systems are upgraded or modified.
- Document physician and staff completion of AI scribe training, including training dates and levels for each staff member.

4. Adopt "built-in" technical safeguards in your EHR system
When using AI scribes that interact with your EHR, explore and use any built-in safeguards for your EHR, such as:

- prompts for a physician to confirm or verify important information, such as medications, dosages, or patient allergies;
- highlighting or "flagging" potential inaccuracies for physician review; or
- requiring physician review of AI-generated content before closing a record.

5. Stay informed about the use of AI in health care

- Keep track of evolving legal and regulatory guidance for AI use in health care.
- Understand how clinical information captured by the AI scribe may be stored, retained, accessed, and subsequently used.
- Consider taking professional development courses or training in appropriate and legal AI use. Document any training or education you receive on AI use.
- Contact your medical professional liability insurer about any AI-specific concerns you may have.

CONCLUSION

AI medical scribes offer significant benefits in reducing administrative burden and potentially reducing physician stress and burnout. However, their

use introduces new liability concerns. Physicians using these tools must remain vigilant in their oversight of these systems and their documentation; establish strong policies and procedures for their safe use; ensure appropriate patient informed consent procedures; and stay informed about developing legal standards for AI use.

SOURCES

1. Henry TA. 2 in 3 physicians are using health AI—up 78% from 2023. American Medical Association. February 26, 2025. Available at https://www.ama-assn.org/practice-management/digital-health/2-3-physicians-are-using-health-ai-78-2023. Accessed May 19, 2025.
2. Reddy Bonguraia A, Save D, Virmani A, et al. Transforming Health Care with Artificial Intelligence: Redefining Medical Documentation. Mayo Clinic Proceedings: Digital Health. Volume 2, Issue 3. September 2024. Available at https://www.sciencedirect.com/science/article/pii/S2949761224000415. Accessed May 15, 2025.
3. Robeznieks A. Five physician specialties that spend the most time in the EHR. American Medical Association. September 11, 2024. Available at https://www.ama-assn.org/practice-management/digital-health/five-physician-specialties-spend-most-time-ehr. Accessed May 19, 2025.
4. Barth S. AI in Healthcare. Foresee Medical. 2018. Available at https://www.foreseemed.com/artificial-intelligence-in-healthcare. Accessed May 19, 2025.
5. Canadian Medical Protective Association. AI Scribes: Answers to frequently asked questions. December 2023. Available at https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2023/ai-scribes-answers-to-frequently-asked-questions. Accessed May 19, 2025.
6. Federation of State Medical Boards. Navigating the Responsible and Ethical Incorporation of Artifical Intelligence into Clinical Practice. Adopted April 2024. Available at https://www.fsmb.org/siteassets/advocacy/policies/incorporation-of-ai-into-practice.pdf. Accessed May 19, 2025.
7. U.S. Department of Health and Human Services. HHS Office for Civil Rights Settles HIPAA Security Rule Investigation with Northeast Radiology. Press release. April 10, 2025. Available at https://www.hhs.gov/press-room/hhs-ocr-hipaa-settlement-nerad.html. Accessed May 19, 2025.
8. American Medical Association. Augmented Intelligence Development, Deployment, and Use in Health Care. November 2024. Available at https://www.ama-assn.org/system/files/ama-ai-principles.pdf. Accessed May 19, 2025.
9. Good C. Sample Patient Consent Form for Using Artificial Intelligence for Dictation, Transcription. Medical Group Management Association. April 2, 2024. Available at https://www.mgma.com/member-tools/sample-patient-consent-form-for-using-ai. Accessed May 19, 2025.
10. Henry TA. 7 tips for responsible use for health care AI. American Medical Association. March 4, 2021. Available at https://www.ama-assn.org/practice-management/digital-health/7-tips-responsible-use-health-care-ai. Accessed May 19, 2025.
11. Vanderpool D. Risk Management: Artificial Intelligence in Clinical Practice. Innovations in Clinical Neuroscience. December 1, 2024. Available at https://pmc.ncbi.nlm.nih.gov/articles/PMC11709444/. Accessed May 19, 2025.
12. Agarwal P, Lall R, Girdhari R. Artificial intelligence scribes in primary care. Canadian Medical Association Journal. September 16, 2024. Available at https://pmc.ncbi.nlm.nih.gov/articles/PMC11412733/. Accessed May 19, 2025.
13. Texas Administrative Code. Rule 163.1 (b) (7). Available at https://texas-sos.appianportalsgov.com/rules-and-meetings?$locale=en_US&interface=VIEW_TAC_SUMMARY&recordId=223450. Accessed June 3, 2025.

Wayne Wenske can be reached at wayne-wenske@tmlt.org.

CLOSED
CLAIM
STUDY

FAILURE TO PROPERLY MANAGE PATIENT'S CENTRAL VENOUS CATHETER

by Laura Hale Brockway, ELS, Vice President, Marketing

This closed claim study is based on an actual malpractice claim from Texas Medical Liability Trust. This case illustrates how action or inaction on the part of the physicians led to allegations of professional liability, and how risk management techniques may have either prevented the outcome or increased the physician's defensibility. This study has been modified to protect the privacy of the physicians and the patient.

PRESENTATION

A 63-year-old woman was hospitalized for treatment of renal and urological issues. Two years earlier, she had been diagnosed with renal cell carcinoma. The patient's history included diabetes, obesity, and breast and colon cancer. The patient lived in a small, rural community.

The patient had seen multiple physicians during her hospitalization, including her long-time physician, Family Physician A. She was discharged to a local rehab center with diagnoses of radiation cystitis, acute renal failure, right renal mass, urinary tract infection, E. coli infection, pneumonia, and splenomegaly. She was to receive IV antibiotics at the rehab center.

PHYSICIAN ACTION

During a visit on day 32 of her rehab stay, Family Physician A documented that the patient had signs of infection in the central venous catheter (CVC). His handwritten note said "septic-unlikely pt apprs well." A typed assessment stated:

"1. Groin area fungal infection 2. Right port-a-cath with hyperemic irritation part of the chest rash or infection secondary to patient already having a lot of skin reaction will treat with only [fluconazole]. 3. Skin reaction. 4. Septic? (Consider this diagnosis in need to transfer to [city], discussed with [son] to help with getting patient to a urologist, patient medical problems could be addressed and patient could get surgery done since it keeps getting postponed, [son] prefers [hospital name] but agrees and other hospital would be ok, not septic."

Family Physician A's plan was to treat the patient with diphenhydramine, cetirizine, and fluconazole. *"Refer to surgery for removal of port-a-cath. Will look for another urologist. Discussed with [son] about accepting another urologist for the renal cancer . . . to hospitalize patient in [city] so that the surgery can occur as soon as possible, if still a candidate."*

Two days passed and rehab center staff advised Family Physician A that the patient had a fever. He told staff to take the patient to a local ED if the fever did not respond to acetaminophen. Following a phone call from the patient's son reporting that the patient had a hard, painful area on her lower right abdomen, Family Physician A instructed rehab center staff to take the patient to a local ED.

The patient was admitted to the hospital that day with "acute septic shock likely secondary to urinary tract infection for Gram negatives; hypotension; acute kidney injury superimposed on chronic kidney disease stage 4 or 5; allergic reaction, Stevens Johnson like type; and renal mass, which is likely cancer."

The next day, the patient was transferred to an urban medical center. Her prognosis was poor, and she died two days after the transfer.

ALLEGATIONS

A lawsuit was filed against Family Physician A. The allegations were failure to discontinue the CVC when it was no longer needed and failure to order cultures and antibiotics if he suspected a CVC infection.

LEGAL IMPLICATIONS

Although physicians who reviewed this case for the defense stated that Family Physician A met the standard of care, there was concern that he did not order cultures or start antibiotics though he noted a possible infection. Reviewers also stated that the order to remove the CVC should have been designated as "STAT."

Regarding causation, one physician reviewer stated that the patient likely had an acute skin condition such as Stevens-Johnson Syndrome or toxic epidermal necrolysis at the CVC site. Further, if the CVC site was infected and that infection became so severe that it caused the patient's death, the site would likely have displayed gross evidence of infection (swelling, redness, warmth, tenderness, etc.). According to this physician, the sepsis, septic shock, and multi-system organ failure that caused the patient's death were "entirely independent" of the CVC.

Documentation was a weakness in this case. Family Physician A testified that although he did not think there was a CVC infection, he documented that there was so the patient could be transferred to an urban hospital and undergo surgery for the renal mass. He stated he was trying to help the family. Yet it was later discovered that the notes about the expedited transfer to an urban hospital were added to the medical record six days after the patient's death.

DISPOSITION

This case was settled on behalf of Family Physician A.

RISK MANAGEMENT CONSIDERATIONS

Physicians who practice in rural areas face unique circumstances that can increase liability risks.

- Limited access to specialists often means primary care physicians manage complex conditions that would typically involve specialty consultation in urban areas.
- Greater distances to specialized care centers can delay transfers when urgent issues arise.
- Fewer resources for diagnostic testing can lead to delayed diagnoses.
- Staffing shortages may cause less frequent patient monitoring.

For physicians practicing in rural communities, developing strong referral networks and clear transfer protocols is essential. Telemedicine can be a valuable tool to bridge some of these gaps, allowing for remote consultation while keeping patients in their communities when appropriate.

Proactive risk assessment — identifying which patients might need more urgent intervention or transfer — can help mitigate these care challenges.

Documentation becomes even more critical when treating patients in these settings, as care coordination between physicians and facilities requires clear communication. However, inaccurate documentation was a factor in this case. Family Physician A's notes were inconsistent with his testimony, and he admitted that he documented an infection that he believed did not exist to facilitate a transfer. Furthermore, the notes regarding the expedited transfer were added to the medical record days after the patient's death.

To maintain the accuracy and integrity of medical records, document patient assessments factually and contemporaneously. Avoid falsifying or exaggerating conditions to achieve secondary goals like transfers. Accurate medical information must be available to all members of the care team and lessens the chance that the facts of the case can be contested.

Avoid making late additions to the medical record after an unexpected outcome. An addendum or late entry in a medical record may be allowed if done in a timely manner and clearly identified. Include the date and time of the addendum, the date and time of the actual encounter, reason for the late entry, the added information, and signature of the author. After-the-fact entries may be viewed as record alterations and may ultimately compromise the defense.

Laura Brockway can be reached at laura-brockway@tmlt.org.

DELAY AND FAILURE TO DIAGNOSE CHOLESTEATOMA

by Wayne Wenske, Senior Marketing Strategist

This closed claim study is based on an actual malpractice claim from Texas Medical Liability Trust. This case illustrates how action or inaction on the part of the physicians led to allegations of professional liability, and how risk management techniques may have either prevented the outcome or increased the physician's defensibility. This study has been modified to protect the privacy of the physicians and the patient.

PRESENTATION

On April 9, 2020, a seven-year-old boy was brought by his mother to see an otolaryngologist (ENT A) on referral from the boy's pediatrician (Pediatrician A).

The patient had a history of frequent ear and throat infections with fluid in his ears, nasal congestion, runny nose, coughing, and occasional snoring. The patient had received speech therapy services up until he was three years old for speech delay.

The patient had undergone an audiogram that showed right conductive hearing loss with fluid in the right ear. The mother was concerned that the ear infections were affecting his ability to hear and contributing to his speech delay.

PHYSICIAN ACTION

ENT A examined the patient and noted fluid in the left ear and tonsils at 2.5+. He recommended tonsillectomy and bilateral myringotomy with tympanostomy. Surgery was scheduled and informed consent was obtained from the patient's mother.

On May 17, ENT A performed the procedures on the patient. During the procedures, ENT A found significant adenoid hypertrophy causing near full obstruction of the nasopharynx. He also performed an adenoidectomy on the patient. No complications were noted. Through the rest of the month, ENT A followed the patient and documented no ear drainage was present, ear tubes remained intact, and the tonsillar bed was healing.

At a follow-up appointment on September 29, the patient's mother reported that his speech was improving. ENT A noted that the patient's ear tubes were visible and open and there was no recurrent ear infection.

At two follow-up appointments over the next eight months, the patient's ear tubes were noted as open and patent with mild severity. An audiology test revealed conductive hearing loss in the right ear and an abnormal eardrum. The patient's mother also reported she was taking her son to a speech therapist.

Hearing tests conducted over the next four months were consistent with initial findings. On April 20, 2021, the patient's mother reported her son's speech development had plateaued.

ENT A diagnosed speech and language delay due to hearing loss, bilateral chronic serous otitis media, allergic rhinitis, and conductive hearing loss of the right ear. ENT A prescribed ciprofloxacin and dexamethasone drops for the right ear.

Follow up audiology testing revealed a Type-B tympanogram of the right ear; the audiologist documented that the right tube was not moving properly. Tests showed conductive hearing loss in the right ear.

ENT A referred the patient to ENT B for a second opinion. On August 12, 2021, ENT B found the right ear to be very far anterior and inaccessible for patency. ENT B discussed with the patient's mother either having the patient's ear tube removed or ordering imaging studies to rule out any tumors or cysts.

The mother chose to move forward with imaging studies, but there was no documentation that these orders were submitted or there was any follow up from ENT B's office or the patient's mother on the studies.

Approximately one month later, the patient was seen by ENT C on referral from Pediatrician A for continued hearing loss after tube placement. ENT C noted right ear effusion without acute infection; no tenderness or swelling of the mastoid; and that the patient could detect voices at a conversational level. Her assessment included a clogged right tympanostomy tube. The patient's mother planned to follow up with ENT A for a possible right tube replacement.

On September 22, ENT A removed the right ear tube from the right anterior inferior ear drum. Five days later, the patient had a hearing test that showed continued hearing loss in the right ear. A tympanogram showed an abnormal right eardrum.

On referral from Pediatrician A, the patient was taken to see ENT D on November 21 for hearing loss. ENT D ordered a CT of the temporal bone to rule out a middle ear mass. A CT performed on December 10 showed a right-sided cholesteatoma with partial

erosion of the ossicular chain and partial dehiscence of the tegmen tympani. ENT D advised that surgery was required.

On February 7, ENT E performed a right tympanoplasty and mastoidectomy and right posterior auricle split-thickness skin graft. Reconstruction surgery was performed on November 12. Recurrent cholesteatoma was found in the sinus tympani and a small external canal cholesteatoma in the anterior sulcus.

A hearing test conducted a year later found the patient's hearing remained essentially stable with a slight decrease in the right ear.

ALLEGATIONS

The patient's family filed a lawsuit against ENT A with allegations of delay and failure to diagnose cholesteatoma resulting in permanent hearing loss.

LEGAL IMPLICATIONS

Expert consultants for both the plaintiff and defense agreed that congenital cholesteatoma is rare, difficult to diagnose, and that a diagnosis is often delayed without persistent conductive hearing loss or a visible mass in the middle ear behind the eardrum. The condition is more likely to develop slowly in adults. The patient was seen by several ENT physicians without a diagnosis of cholesteatoma.

One defense expert stated that the cholesteatoma would not have been seen by the various ENTs treating the patient because of its location. The cholesteatoma was in the posterior aspect of the middle ear near the ossicles. The expert explained that when one looks in the ear with a scope, the anterior aspect is the only visible part of the ear. This expert added that a CT immediately after myringotomy would also not have found the cholesteatoma due to its location and size (being too small and not visible).

An otolaryngology consultant for the defense believed that the patient's hearing loss was caused by ossicular chain damage from cholesteatoma that had occurred before the patient was seen by ENT A. This consultant felt it was not reasonable to expect ENT A to suspect cholesteatoma in a young child. Instead, given the patient's symptoms, age, and number of ear infections, it was reasonable and "within the standard of care" for ENT A to remove the tonsils and place ear tubes.

This consultant did point out that there was a delay in obtaining imaging studies to rule out tumors or cysts. There was no documentation by ENT A or ENT B that these tests were ordered. While overall care provided to the patient was appropriate, earlier imaging may have identified the cholesteatoma sooner.

An expert consultant for the plaintiff could not make a causal link from ENT A's care of the patient to specific damages. He could only testify that "an earlier diagnosis would have been better."

DISPOSITION

This case was taken to trial, and the jury returned a verdict in favor of the plaintiffs.

RISK MANAGEMENT CONSIDERATIONS

In this case, the patient's young age may have been a factor in the diagnosis delay — and the sympathies of the jury. When treating minors, the normal physiological and developmental changes that occur in the patient over time may contribute to a delayed or missed diagnosis, especially in the event of a rare condition such as congenital cholesteatoma.

ENT A and B were both criticized for not obtaining imaging studies that may have identified the cholesteatoma in a timelier manner. When recommending and agreeing to diagnostic tests for a patient, it is the physician's responsibility to order the test; document the order; obtain the test results in a timely manner (if the patient is compliant); review the results when received; document his or her review in the medical record; and initiate appropriate follow up with the patient.

Had imaging studies been obtained earlier in this case, the patient's cholesteatoma may have been diagnosed earlier. It was unclear why the tests discussed with the mother were not ordered. If a patient or parent decides not to proceed with a recommended test, their decision should be documented in the medical record.

To avoid risks associated with a failure to follow up, physicians may consider establishing clear policies and procedures for patient follow up. Adopt technologies in the electronic health record (EHR) system that employ built-in systems such as reminders for testing or alerts when results of ordered testing have not been received. Consider prioritizing test results with "urgent," "critical," "action needed," or "pending results."

There was also concern that ENT A made documentation errors in the patient record, such as mistaking whether the patient's right or left ear was affected. There were also patient visit notes that were added to the record up to a week after the patient was seen.

Clear, contemporaneous documentation helps to ensure that critical data is available to all treating health care providers and helps to maintain continuity of care. Together, timely consults, testing, and comprehensive medical records, that are accessible by the entire care team, can help catch potential diagnostic errors or oversights before they negatively affect patient outcomes.

Wayne Wenske can be reached at wayne-wenske@tmlt.org.

Coming soon to your email inbox ...

the all-new digital Reporter

We're going digital. Our quarterly publication, *the Reporter*, is moving fully online with the same features, CME, closed claim studies, and information you've come to expect from TMLT. But now we're adding exciting digital features, specifically to be accessed online, such as videos, interactive polls, and more timely health care news, trends, and updates.

Be on the lookout for the third quarter edition coming this fall — to your mobile phone, tablet, laptop, or desktop.

Read. Download. Share.

www.tmlt.org/reporter

the REPORTER

Pre-sorted Standard
U.S. Postage
PAID
Permit No. 90
Austin, Texas

TEXAS MEDICAL LIABILITY TRUST
P.O. Box 160140
Austin, TX 78716-0140
800-580-8658 or 512-425-5800
www.tmlt.org

JOIN US
ON SOCIAL
MEDIA

FACEBOOK: TexasMedicalLiabilityTrust
INSTAGRAM: TexasMedicalLiabilityTrust
LINKEDIN: TMLT

TMLT
Texas Medical Liability Trust