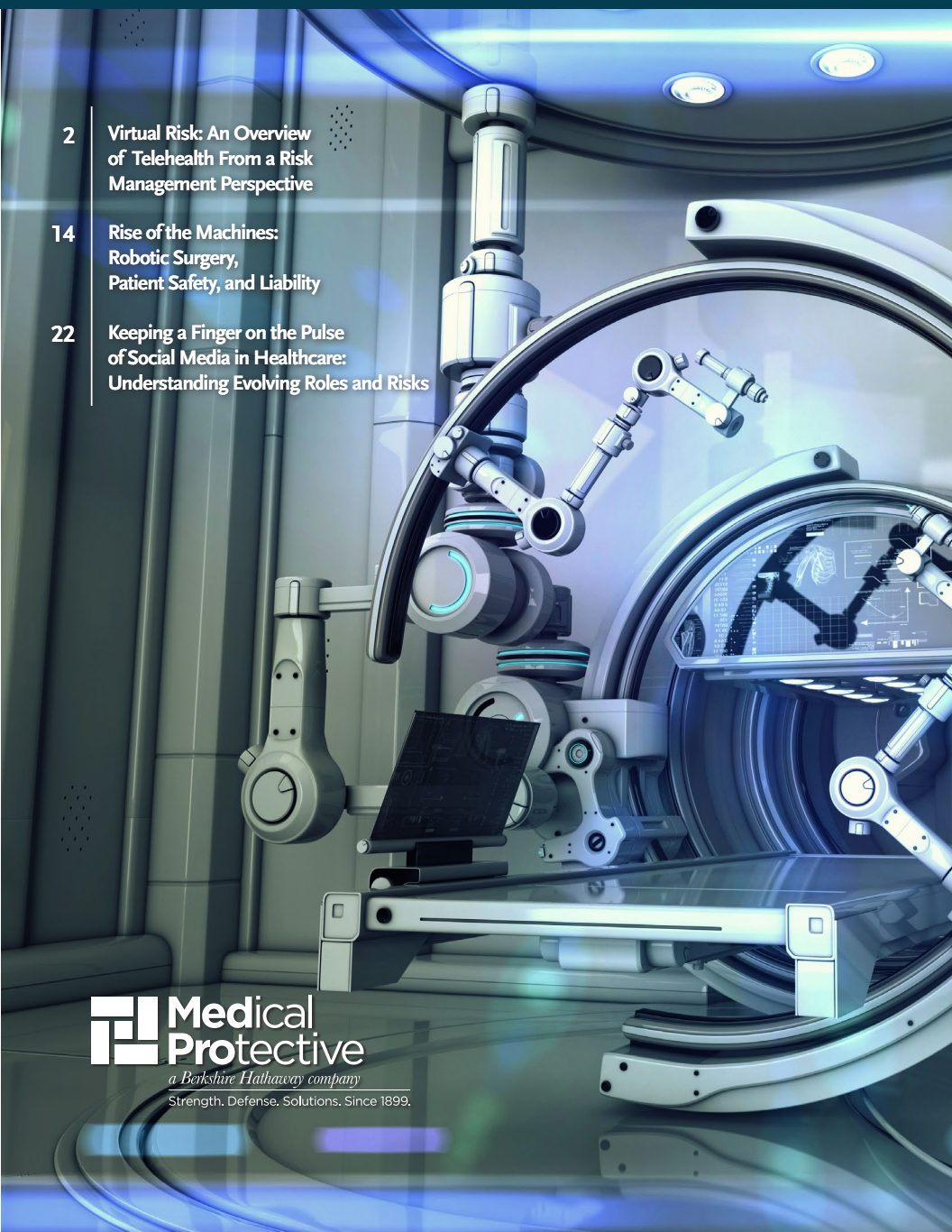
Volume 95 ■ Number 1 ■ Spring 2014

PROTECTOR

Setting clinical risk management standards since 1913.



Medical Protective

a Berkshire Hathaway company

Strength. Defense. Solutions. Since 1899.

Protector Continuing Education Program

Medical Protective is pleased to offer a free resource for Continuing Education (CE) hours for our insureds. *Protector* is published three times each year. In order to obtain 1 hour of free CE, you must read the most recent *Protector* and then complete the applicable online test – which can be accessed by logging on with your username and password at www.medpro.com or visiting http://www.medpro.com/protector-ce.

Allow sufficient time to complete the test in one sitting, as information that is not submitted cannot be saved. Upon submission of a test, you will immediately receive a pass/fail notification. If you pass with a minimum score of 80 percent, you will also receive a certificate that you should retain in your CE file. If you fail, you cannot retake that particular test. Each test will be available for approximately 4 months, until the next issue of *Protector* is published.

Osteopathic physicians, nonphysician doctors, and advanced practice healthcare professionals can submit certificates to their professional associations for review.

Medical Protective is accredited by the Accreditation Council for Continuing Medical Education to provide continuing medical education for physicians.

Medical Protective designates this journal-based CME activity for a maximum of 1 AMA PRA Category 1 Credit.™ Physicians should claim only the credit commensurate with the extent of their participation in the activity. This activity was planned and produced in accordance with the Essentials and Standards of the ACCME.

The Medical Protective Company is designated as an Approved PACE Program Provider by the Academy of General Dentistry. The formal Continuing Dental Education programs of this program provider are accepted by AGD for Fellowship/Mastership and membership maintenance credit. Approval does not imply acceptance by a state or provincial board of dentistry or AGD endorsement. The current term of approval extends from October 1, 2011 to September 30, 2015. The Medical Protective Company designates this Continuing Education activity as meeting the criteria for up to 1 hour of Continuing Education credit. Doctors should claim only those hours actually spent in the activity.

If you pass two tests within 1 year, you also may be eligible to earn a 1-year risk management premium credit, which will be applied automatically at your next policy renewal.*

This journal-based Continuing Education activity was developed by Medical Protective without commercial support. Continuing Education planners, content developers, editors, committee members, and Medical Protective Clinical Risk Management staff report that they have no relevant financial relationships with any commercial interests.

* LIMITATIONS: Every effort has been made to ensure that *Protector* content is applicable to the risk management learning needs of all healthcare professionals. Approval by ACCME or AGD does not imply acceptance by any other accrediting body. It is the healthcare professional's responsibility to ensure that courses are accepted by their respective licensing boards or accrediting bodies. Premium credit eligibility and amount are subject to business and regulatory approvals and may vary by policy type. Due to state filing restrictions, the premium credit associated with the *Protector* Online Continuing Education test is not available for physicians in Alaska; however, insureds in this state are still eligible for the free CE hours. Doctors who are less than 18 months into receiving a risk management premium credit are welcome to complete the *Protector* test for CE hours, but a further premium credit will not be earned. Doctors who are 18 months or more into receiving a risk management premium credit can take the *Protector* test to earn premium credit toward a future renewal. Completion of a risk management course does not imply or guarantee renewal.

The Medical Protective website is best viewed in Internet Explorer 8 and higher or Firefox 3.5 and higher. If you have questions, please contact the Clinical Risk Management Education team at (800) 463-3776.

Dear Healthcare Provider:

As physicians and dentists know all too well, increasing demands and competing priorities in healthcare have resulted in considerable challenges in recent years. To address these challenges, the healthcare community is continually looking for new and innovative ways to transform the delivery of care.

In 2013, *Protector* examined two pivotal ways in which this is happening: (1) through the use of electronic health records (EHRs), and (2) through increasing emphasis on alternative workforce models. This edition of *Protector* will focus on other technologies — telehealth, robotic surgery, and social media — that are helping revolutionize the practice of medicine and dentistry and redefine care delivery and communication.

Although these technologies create new opportunities and benefits for patients and providers, their use also introduces new challenges and risks related to licensing, training, credentialing, informed consent, privacy/security, and more.

By reading the articles in this issue of *Protector*, you should be able to:

- Cite barriers and risks associated with telehealth, and describe several strategies that can help address telehealth liability concerns;
- Explain why training, learning curve, and proficiency are top risk concerns for robotic surgery; and
- Identify key areas for consideration in the development of social media policies.

As a reminder, Medical Protective is accredited to provide Continuing Education (CME or CDE) hours for physicians and dentists. One of the ways to earn CME or CDE credits is by taking a test after reading this issue of *Protector*. Online access will make it easy for you to complete the test that accompanies this issue.

MedPro insureds who pass two tests in the same policy year might be eligible to earn premium credits. For more information, please review the inside cover of this issue. Or, visit our website at www.medpro.com.

As always, your comments and suggestions are welcome.

Sincerely,

Laura M. Cascella

Laura M. Cascella, MA
Clinical Risk Management Writer/Editor

Virtual Risk: An Overview of Telehealth From a Risk Management Perspective

Laura M. Cascella, MA

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

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

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

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

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

Why Telehealth?

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

Both the dental and medical communities have recognized telehealth as an up-and-coming area of practice.

Both the dental and medical communities have recognized telehealth as an up-and-coming area of practice. In 2011, the American Dental Association's House of Delegates adopted a resolution that directed its Council on Dental Practice to spearhead an evaluation of teledentistry in dental practices.[2]

In 2012, the Institute of Medicine explained that the role of telehealth is becoming more important "as we move away from the traditional fee for service system and toward new models of care, including accountable care organizations (ACOs), patient-centered medical homes (PCMHs), and other strategies that focus on outcomes."[3]

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

- Improved access to care and resources for patients in rural areas or areas that have provider shortages;
- Lower costs and improved efficiency as a result of pooling resources, reducing travel time, and better managing patient care;
- Comparable or improved quality of care; and
- Increased patient satisfaction, which may occur as a result of better access to care, convenience, and reduced stress.[4]

How Is Telehealth Regulated?

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

The Telehealth Policy Resource Center, a program of the Health Resources and Services Administration (HRSA), notes that as mobile technologies emerge, additional federal agencies will likely have jurisdiction, including the Federal Trade Commission (FTC), the Federal Communication Commission (FCC), and the Department of Health and Human Services (HHS).[5]

State legislatures and state medical and dental boards also play a significant role in determining telehealth standards and boundaries within individual states, including licensure requirements,

Telehealth Technologies

Telehealth doesn't describe one particular service or technology; rather, it refers broadly to the ways in which telecommunication is integrated into healthcare delivery.

Some of the most common telehealth applications are:

- Videoconferencing, which is used for real-time interactions among providers and between providers and patients;
- Store-and-forward imaging, which is used to send images and recordings from one provider or organization to another for later review (not real-time);
- Remote patient monitoring, which uses electronic devices to transmit patient health data from the patient's location (e.g., home or a healthcare facility) to providers at a distant site;
- Mobile technology (also called mHealth), which uses smartphones, tablets, portable monitoring sensors, and other mobile devices to send health information or provide patient services; and
- Robot-assisted services, in which providers at remote locations use robots to monitor patients, perform surgery, and more.

scope of practice parameters, and issues concerning reimbursement.

Healthcare providers and organizations participating in telehealth programs should be cognizant of state telehealth laws, practice acts, and standards of care for each state in which they plan to practice.

Although the use of telecommunications in healthcare is not new, it is only now becoming more widespread. Thus, many states may not yet offer specific laws or detailed guidance on telehealth activities. As telehealth becomes more common, providers can expect to see more defined state and federal policies.

What Are the Risks and Barriers Associated With Telehealth?

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

Licensing

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

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

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

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

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

To learn more about the statutes and regulations in the state(s) in which you practice, visit http://telehealthpolicy.us/state-laws-and-reimbursement-policies or contact the state's medical board or dental board.

Credentialing and Privileging

Credentialing and privileging — the processes by which an organization or practice assesses and confirms the qualifications of a healthcare provider and authorizes the provision of specific services —[9] play an important role in patient safety and quality care. This is equally true for both traditional, in-person care and telehealth services.

The ECRI Institute explains that while remote practitioners will not have the same relationship with a healthcare facility as do onsite providers, the facility still must exercise the same level of due diligence in its screening and selection processes. They must ensure that the distant site practitioner is legally allowed to provide care to the specified patient population, and that he or she is qualified for the scope of services requested.[10]

Since 2011, CMS has allowed the governing body of an organization whose patients are receiving telehealth services to rely on credentialing and privileging decisions made by a distant site hospital or "telemedicine entity," such as a teleradiology group or ambulatory surgery center. This is known as "credentialing by proxy." Credentialing by proxy helps organizations save time and money, but certain requirements must be met, such as a written contract between the originating and distant sites.[11] For more information, visit http://telehealthpolicy.us/credentialing-privileging.

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

Online Prescribing

Online prescribing refers to a "provider's ability to prescribe drugs to a patient who has been diagnosed and treated via telehealth."[12] Online prescribing is different from e-prescribing, which simply refers to a provider's ability to send prescriptions electronically to a pharmacy, but does not account for whether the patient was seen in person or using telecommunication technology.

When it comes to prescribing medications, lack of physical interaction creates patient safety and liability concerns.

Technology has, in certain circumstances, eliminated the need for the face-to-face visits that are typical in traditional medical and dental care. However, when it comes to prescribing medications, lack of physical interaction creates patient safety and liability concerns. In fact, the Center for Telehealth & e-Health Law notes that "the majority of legal actions that have been brought against telehealth providers proceeded as a result of telemedicine practitioners prescribing medications over the internet, rather than actions having been brought because care was negligently administered through telemedicine."[13]

Major concerns related to online prescribing include whether an appropriate provider–patient relationship has been established, whether the doctor has been able to adequately assess the patient, and whether the patient has provided an accurate health history.

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

Federal prescribing regulations. CMS addresses e-prescribing as part of its Medicare rules, and the DEA addresses online pharmacies and telemedicine as part of the Controlled Substances Act. Further, the 2008 Ryan Haight Online Pharmacy Act — named for a teenage boy who died after overdosing on pain medication prescribed by a doctor whom he had never seen — prohibits the distribution of controlled substances via the Internet in the absence of a valid prescription. The validity of a prescription is based on whether a practitioner examined the patient in person, "with certain exceptions for telemedicine activities."[14]

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

- Put restrictions on how the provider–patient relationship is defined;
- Require doctors to have a preexisting relationship with the patient in order to engage in online prescribing;
- Require a face-to-face physical exam prior to online prescribing, and whether the exam can be performed using a telehealth medium, such as videoconferencing;
- Prohibit questionnaires and surveys as the sole basis for online prescribing; and/or
- Have other requirements related to patient medical history, written documentation, appropriate follow-up care, and emergency provisions.[15]

State-specific information about online prescribing can be obtained from state medical and dental boards. For general information about online prescribing, visit the Telehealth Policy

Case Example

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

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

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

The doctor ultimately pleaded no contest to the felony charge; he was sentenced to 9 months in county jail and ordered to pay more than $4,000 to the court and state B's medical board.

Resource Center at http://telehealthpolicy.us/online-prescribing or the Telehealth Resource Centers at http://www.telehealthresourcecenter.org/toolbox-module/online-prescribing-and-telepharmacy.

Informed Consent

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

Medical Protective's *Informed Consent* guideline explains that "any procedure that presents the possibility of material harm to a patient should not be undertaken until the informed consent process has been completed. The thoroughness and complexity of the informed consent process will depend on the degree of risk that accompanies the procedure."[16]

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

A recent article about informed consent and telehealth states that "in the practice of telehealth, reliance on imperfect technological tools, as well as the 'distance' factor, can propel otherwise routine treatments into a higher risk category."[17] Risks specific to telehealth include technological glitches and failures (including transmission errors), technology-related privacy and security concerns, and lack of hands-on patient evaluation.

In telehealth, the informed consent process must also take into account risks specific to the delivery of care using telecommunication technologies.

As telehealth has become a more viable option for healthcare delivery, a handful of states have implemented informed consent laws that pertain specifically to telehealth.[18] As with licensure, informed consent laws vary between states. For example, some states may require written informed consent, while others permit verbal consent.

Even in the absence of state guidance, telehealth providers should carefully consider their use of an informed consent process. As the aforementioned article notes, "failure to properly obtain a patient's informed consent before initiating telehealth services can increase a provider's risk of facing consent-based negligence claims . . ."[19]

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

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

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

The transmission of data to and from various locations increases the risk of inappropriate disclosure and data breaches.

Privacy/Security

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

For example, the transmission of data to and from various locations increases the risk of inappropriate disclosure and data breaches. Thus, healthcare practices and organizations must implement privacy and security safeguards at all points of exposure, including at the originating site, across the transmission medium, and at the distant site.[20] Examples of these safeguards include data encryption, user authentication, password security, patient verification technologies, protected wireless networks, data tracking and auditing, and more.

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

Specifically, the HIPAA omnibus rule that was published in January 2013 sets forth standards related to electronic PHI and requires covered entities and business associates to implement policies and procedures "to prevent, detect, contain, and correct security violations," inclusive of risk analysis and risk management activities.[21]

When working with vendors who supply telehealth services or equipment, healthcare practices and organizations should determine whether the vendors are considered business associates per HIPAA standards. A business associate "is a person who . . . creates, receives, maintains, or transmits protected health information for a function or activity regulated by [45 CFR, Subtitle A, Subchapter C]."[22]

If a vendor qualifies as a business associate, the practice and vendor should have a business associate agreement

(BAA) in place. The agreement should outline appropriate use and disclosure of PHI by the vendor to ensure security. For more information about business associates and a sample BAA, visit http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Healthcare practices and organizations also should consider their policies related to security of mobile devices, use of social media, appropriate technologies and applications (apps), and electronic communication with patients. A risk analysis that takes into account the services offered, the method of delivery, and the types of technologies involved can help practices identify areas of exposure and take action to address them.

A risk analysis that takes into account the services offered, the method of delivery, and the types of technologies involved can help practices identify areas of exposure and take action to address them.

For additional guidance on risk analysis requirements under HIPAA, visit http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

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

What Are the Malpractice Trends Related to Telehealth?

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

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

In addition to managing general risk concerns, practitioners may face other uncertainties specifically related to the provision of care via telecommunications. For example, because standards and regulations for medical malpractice vary by state, telehealth programs and services that cross state lines may create legal concerns pertaining to jurisdiction, procedure, choice of state law, and standards of care.[23]

Further, the ECRI Institute notes that lawsuits involving telehealth "are more likely to target numerous defendants and involve more than one theory of liability."[24] A telehealth-related lawsuit may name providers at the originating and distant sites, as well as their healthcare facilities, as defendants. A lawsuit also could potentially implicate telecommunication vendors and their consultants.

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

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

...because standards and regulations for medical malpractice vary by state, telehealth programs and services that cross state lines may create legal concerns pertaining to jurisdiction, procedure, choice of state law, and standards of care.

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

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

Are You Covered?

When starting a telehealth program or considering participating in telehealth initiatives, it's important to know whether your professional liability insurance provides coverage for these activities. Your insurance agent or broker can help answer questions about policy coverage for telehealth services. If you do not have an agent or broker, contact Medical Protective at 800–4MEDPRO (1–800–463–3776) and ask for assistance with this coverage issue.

Conclusion

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

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

Endnotes

1 Telehealth Policy Resource Center. (n.d.). What is telehealth? Retrieved from http://telehealthpolicy.us/what-telehealth

2 Soderlund, K. (2011, November 21). Resolution calls for study of teledentistry in dental practice. *ADA News*. Retrieved from http://www.ada.org/news/6590.aspx

3 The Institute of Medicine. (2012). *The role of telehealth in an evolving health care environment: Workshop summary*. Washington, DC: The National Academies Press.

4 American Telemedicine Association. (n.d.). What is telemedicine? Retrieved from http://www.americantelemed.org/learn/what-is-telemedicine; ECRI Institute. (2012, May). Telemedicine. *Healthcare Risk Control, 3;* Soderlund, Resolution calls for study of teledentistry in dental practice.

5 Telehealth Policy Resource Center. (n.d.). Mobile health. Retrieved from http://telehealthpolicy.us/mobile-health

6 ECRI Institute, Telemedicine; Youngstrom, N. (2012, March 19). With use of telehealth expected to grow, hospitals confront fraud, HIPAA pitfalls. Atlantic Information Services. Retrieved from http://aishealth.com/archive/rmc031912-02

7 Kepler, T., & McGinty, C. L. (2009). Telemedicine: How to assess your risks and develop a program that works. American Health Lawyers Association. Retrieved from http://www.healthlawyers.org/Events/Programs/Materials/Documents/HHS09/kepler_mcginty.pdf

8 Natoli, C. M. (2009, December). Summary of findings: Malpractice and telemedicine. Center for Telehealth & e-Health Law. Retrieved from http://ctel.org/library/research/

9 Health Resources and Services Administration. (2001, revised 2006). Credentialing & privileging of health center practitioners. Policy Information Notice 2001-16. Retrieved from http://bphc.hrsa.gov/policiesregulations/policies/pin200116.html

10 ECRI Institute, Telemedicine.

11 Telehealth Policy Resource Center (n.d.). Credentialing & privileging. Retrieved from http://telehealthpolicy.us./credentialing-privileging

12 Telehealth Policy Resource Center. (n.d.). Legal issues. Retrieved from http://telehealthpolicy.us./legal-issues

13 Natoli, Summary of findings: Malpractice and telemedicine.

14 Kepler, et al. Telemedicine: How to assess your risks.

15 Telehealth Policy Resource Center. (n.d.). Online prescribing. Retrieved from http://telehealthpolicy.us./online-prescribing; Youngstrom, With Use of Telehealth Expected to Grow.

16 The Medical Protective Company. (2012). *Informed Consent*. Fort Wayne, IN: Medical Protective.

17 Scott, B. (2013, June 19). Proactively approaching telehealth informed consent. Lexology. Retrieved from http://www.lexology.com/library/detail.aspx?g=a90e1cd6-8090-481b-90c0-7b19407a70a0

18 Kepler, et al. Telemedicine: How to assess your risks.

19 Scott, Proactively approaching telehealth informed consent.

20 ECRI Institute, Telemedicine.

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

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

23 Telehealth Resource Centers. (n.d.) Medical malpractice and liability. Retrieved from http://www.telehealthresourcecenter.org/toolbox-module/medical-malpractice-and-liability

24 ECRI Institute, Telemedicine.

TOP 10
Risk Strategies for Telehealth

1. Be aware of federal and state laws and regulations related to telehealth, such as requirements for licensure, online prescribing, informed consent, clinical decision-making, and quality improvement. Check with your state medical or dental board for specific guidance.
2. Identify and implement telehealth best practices, and stay abreast of any changes in telehealth regulations and standards of care. The American Telemedicine Association and other professional associations have published a number of telemedicine practice guidelines.
3. Ensure that telehealth providers at remote sites are properly credentialed (either by the originating site or the distant site) and qualified for their proposed scope of services. Any privileges granted should comply with applicable scope of practice laws.
4. Develop and implement patient selection criteria and standardized clinical protocols as appropriate to ensure consistency, quality, and efficiency of telehealth services.
5. When multiple providers are involved in a patient's care, have a clear understanding of duty of care and clinical responsibilities, including disclosure of any adverse events. Make sure the specific provisions are documented.
6. Implement protocols to ensure that communication from telehealth providers is promptly reviewed and acted upon.
7. Ensure that technology and equipment used for telehealth services is functional and properly maintained and serviced. Providers and staff should be aware of who is responsible for equipment maintenance.

8. Assess the privacy and security risks of your telehealth systems, and implement safeguards at all points of risk exposure. Monitor the systems for possible security breaches.
9. Train telehealth providers and staff on applicable telecommunication technologies, scope of telehealth services offered, equipment maintenance, and privacy/security standards.
10. Ensure that the organization's mechanism for incident reporting supports telehealth events, and evaluate telehealth activities as part of ongoing quality improvement initiatives. Surveys or questionnaires can help gauge provider and patient satisfaction with telehealth services.

Rise of the Machines:
Robotic Surgery, Patient Safety, and Liability

Laura M. Cascella, MA

The turn of the 21st century was witness to a significant technological milestone in American healthcare — the approval of the first robotic surgical system (RSS) by the U.S. Food and Drug Administration. Now, more than a decade later, robotic surgery is used for hundreds of thousands of procedures in the United States each year, and the number continues to grow.[1]

...the number and types of procedures done using robots have continued to expand over the years, reaching various specialties...

Unlike in open surgery or traditional laparoscopy, in which the surgeon stands over the patient and uses his or her hands to operate the surgical instruments, robotic surgery uses a computer-assisted robot as an intermediary in the surgical process. The surgeon sits at a console and uses hand and foot controls to maneuver instruments and a small camera on thin robotic arms through small incisions in the patient. The surgeon is able to monitor progress using a three-dimensional viewer on the console.

During robotic surgery, the surgeon typically is in the operating room, but removed from the patient. However, the technology also offers the possibility of robotic telesurgery, in which the surgeon operates the robot from a remote location.[2]

Since its inception, robotic surgery has become a "symbol of medical progress," and has been featured prominently in popular print and electronic media.[3] Both large and small healthcare organizations have invested in RSS technology, and the number and types of procedures done using robots have continued to expand over the years, reaching various specialties such as general surgery, urology, gynecology, cardiology, orthopaedics, and oral and maxillofacial surgery. With time, more applications for robotic surgery will most certainly emerge. For example, in dentistry, robots might be used to perform preventive, restorative, and curative procedures.[4] Further, robots "could offer dentistry improved accuracy, predictability, safety, quality of care and speed of treatment."[5]

"Like all new technologies in healthcare, RSS comes with emerging risks. Medical Protective's specialty advisory boards have explored several areas of high risk with regards to robotic surgery. These include training and proctoring, patient selection, adverse events and lessons learned, and quality monitoring and tracking."

— Dr. Graham Billingham,
Chief Medical Officer
Medical Protective

However, despite the growing interest in, and proven and purported benefits of, robotic surgery — such as greater precision and visualization, smaller scars, faster recovery, lower infection rates, and less pain — questions have arisen about patient safety and the appropriate use of this technology. A 2012 article in *Trial*, a publication of the American Association for Justice, states that "RSS are so new that patients, doctors, hospitals, insurers, manufacturers, and the FDA are still trying to determine their efficacy and risks."[6]

This *Protector* article examines some of the risk management concerns surrounding RSS — such as training, competency, credentialing, learning curves, proficiency, patient selection criteria, and informed consent — and offers strategies to help doctors minimize potential liabilities.

Reconciling Business With Safety and Efficacy

For many hospitals and healthcare organizations, the incentive to invest in RSS is significant. Robots have been marketed as a way to increase revenue and capture market share. The technology can offer a state-of-the-art advantage over competitors and provide an enticing recruitment tool for sought-after surgeons.

Further, direct marketing to patients has resulted in increasing pressure for hospitals to offer the cutting-edge robots as a treatment option. The authors of an article about anesthetic care in robotic surgery explain that, "In today's information age, patients are more educated about their options and often have a strong desire to seek out the most advanced therapies, which makes the existence of a robotic program a marketing tool."[7]

However, those who are cautious about RSS point to the limited research comparing robotic surgery outcomes with open surgery and traditional laparoscopic surgery. For example, in March 2013, the Massachusetts Board of Registration in Medicine issued a robot-assisted surgery advisory to its hospitals. Although the board acknowledged that RSS offer numerous technical advantages, they cautioned that large-scale, high-quality, prospective studies have not yet been done.[8]

A spike in RSS-related adverse events reported to the FDA's Manufacturer and User Facility Device Experience (MAUDE) database also has raised concerns. Between 2012 and 2013, the number of adverse event reports linked to robotic surgery more than doubled,[9] accompanied by a proliferation of national and regional media reports detailing deaths and injuries associated with RSS.

Additionally, and as a possible result of the media reports, a simple Internet search of robotic surgery lawsuits turns up numerous law firms seeking clients who have suffered complications or poor outcomes following surgery, such as burns, tearing of the intestines and arteries, organ and nerve damage, excessive blood loss, and bowel injuries.

...because the robots carry a hefty price tag... it will be important for organizations to see a return on their investments...

Although the FDA notes that the increase in adverse event reports might be associated with greater use of robotic surgery and more public awareness,[10] these reports still highlight the need for healthcare organizations and surgeons using RSS to evaluate risks and take necessary precautions to maximize patient safety and minimize liability exposure.

Evaluating Robotic Surgery From a Risk Management Perspective

As the RSS market continues to surge and patient demand grows, more hospitals and healthcare organizations will likely invest in these systems. Further, because the robots carry a hefty price tag — costing between $1.5 and $2.3 million[11]— it will be important for organizations to see a return on their investments, which may result in increased pressure on surgeons to use RSS.[12]

Robotic surgery may potentially offer many benefits for both patients and doctors; however, like any new technology, it also faces challenges, and "questions remain about clinician learning curves, what the ideal training program is, how many procedures are needed to maintain proficiency, and what criteria hospitals should use to credential surgeons using these systems."[13] Additionally, issues related to patient selection, marketing, and informed consent and decision-making have surfaced as primary risk concerns.

Training

This past fall, the ECRI Institute released its list of top 10 health technology hazards for 2014. Number nine on the list was "Robotic Surgery Complications due to Insufficient Training," which noted that RSS are being used with more frequency and for additional types of surgery without consideration of surgical teams' training and proficiency.[14]

ECRI's list supports the notion that training has been, and continues to be, one of the top ongoing risk concerns for robotic surgery — in part because no universal consensus has been reached on the appropriate type and duration of training, and requirements vary widely between facilities.[15]

...training...continues to be one of the top ongoing risk concerns for robotic surgery.

Although product and technical training is offered through the device manufacturer, recent literature suggests that this training alone may not sufficiently prepare doctors to perform surgery with the robot.[16] Ultimately, hospitals and healthcare organizations are responsible for determining their own standards for clinical training, proctoring and oversight, competency, and credentialing.

Guidance from professional associations and information from robotic surgery research studies and literature can help organizations establish appropriate criteria. Several recent research studies and systematic reviews focusing on robotic surgery call for training that (a) is based on competency rather than time or quantity, (b) uses graduated learning objectives, with assessment at each level, (c) involves simulation/virtual training, and (d) sets minimum criteria for demonstrating competency.[17]

A consensus statement from the Society of American Gastrointestinal and Endoscopic Surgeons (SAGES) and the Minimally Invasive Robotic Association (MIRA) describes a broad twofold approach to training that involves technical and capability training and training for specific procedures. The consensus statement further explains that surgeons must have a thorough knowledge base and practical experience, understand standard operating procedures and emergency protocols, and be able to anticipate risks and develop appropriate responses.[18]

For example, surgeons must be prepared to convert to traditional laparoscopy or an open procedure in the event of technical problems or certain clinical complications. As the SAGES-MIRA statement explains, "The basic premise is that the surgeon(s) must have the judgment and training to safely complete the procedures as intended, as well as have the capability of immediately proceeding to an alternative therapy when circumstances so indicate."[19]

Case Example

The complexities involved in converting from robotic surgery to traditional surgery can increase patient risks. In a recent case, surgeons performed a robot-assisted hysterectomy on a patient who was morbidly obese. Complications during the surgery forced the doctors to convert to traditional laparoscopy and, finally, to open surgery. Following the surgery, the patient complained of arm pain, weakness, and numbness, and she was diagnosed with brachial plexus injuries. A review of the case determined that the lengthy duration of the procedure, the patient's obesity, and her positioning prior to the open surgery (in a steep head-down position) contributed to her injuries.

For doctors whose primary surgical experience is using RSS, conversion to open surgery may be problematic. In these cases, another surgeon who is experienced with open surgery should be available to assist if necessary.[20] Surgeons also must be aware of the risks that may occur as the result of converting to traditional surgery — such as issues related to patient positioning and prolonged use of anesthesia — and have plans in place to manage those risks.[21]

Case Example

Lack of defined training standards and limited awareness of the learning curve for robotic surgery have played a role in recent malpractice lawsuits. In one case, a surgeon performed unsupervised prostate surgery on a patient after only two previous supervised robotic prostate surgeries. The surgery took more than 13 hours and resulted in multiple injuries and severe blood loss, as well as the need to convert to open surgery during the process. The complications from the surgery were alleged to have contributed to the patient's death several years later.

Running drills with the surgical team that simulate the appropriate steps to take during an emergency — such as disengaging the RSS, moving it away from the patient, and initiating a conversion to open surgery — can help prepare team members to handle various situations that might arise. Further, lessons learned from drills and actual surgeries can provide the foundation for the development of robotic surgery best practices and protocols.

Learning Curve

In addition to training considerations, surgeons should be aware of the learning curve associated with using RSS. In a recent FDA survey of a small sample of surgeons who are experienced with robotic surgery, all participants stated that they had to perform numerous surgeries using the robot before achieving proficiency. Although they did not think that the complexity of the device was a major barrier, many noted that it took time to learn how to use the foot pedals, acquire needed hand–eye coordination, and operate the platform.[22]

Unfortunately, attaining proficiency with a surgical robot is not a clear-cut issue. The number of procedures required to demonstrate proficiency varies based on the type of procedure, and no firm standards have been set. Some estimates suggest that it may take hundreds of surgeries to attain high proficiency, while other estimates are lower.[23] Further, a number of other factors also contribute to proficiency, such as basic skill, experience with technology, familiarity with the procedure, frequency of cases, and type of training.

Just as with other types of surgery, robotic surgery skills are honed over time. For less experienced surgeons, procedures may take longer and the risk of complications may be higher.[24] Proctoring and mentoring opportunities, established as part of an organization's credentialing guidelines, can help contribute to patient safety initiatives and address risks related to learning curve and proficiency.

Organizational policies also should establish criteria for maintaining proficiency over time, such as performance monitoring, continuing education, training, and recredentialing.

Patient Selection Criteria

One of the driving factors in the rise of robotic surgery is patient demand, but some patients who are eager for this new technology might not be ideal candidates due to comorbidities or other factors. For example, in the prostate surgery case mentioned on page 18, the patient was obese, diabetic, and had a history of heart surgery. These health conditions, combined with the surgeon's limited RSS experience, may have ultimately contributed to the patient's poor outcome.[25]

One of the driving factors in the rise of robotic surgery is patient demand, but some patients who are eager for this new technology might not be ideal candidates due to comorbidities or other factors.

Thus, an important strategy for managing robotic surgery risk is careful consideration of patient selection criteria. All participants in the FDA's 2013 survey of experienced robotic surgeons felt that appropriate selection criteria played a pivotal role in successful patient outcomes. Although they noted that criteria may vary across specialties, standards were primarily based on maintaining patient safety.[26]

The 2013 advisory from the Massachusetts Board of Registration in Medicine also emphasized the importance of establishing patient selection criteria, noting that "Careful preoperative assessment of patient risk is critical for preventing perioperative complications. Both the patient's comorbidities and the complexity of the robotic surgical case are important risk factors that should be considered."[27]

By developing greater awareness of potential risk factors and contraindications for robotic surgery, healthcare organizations and surgeons can create and implement patient selection guidelines and assessment protocols, as well as reinforce or improve quality measures.[28] Further, documenting the assessment of patient risks in accordance with established selection criteria can help justify clinical decision-making.

Another crucial risk strategy is managing patients' expectations related to robotic surgery, which may prove challenging for healthcare organizations and surgeons. Because robotic surgery is new and complex, direct claims about benefits and safety might be difficult to make.

Also, aggressive marketing — such as promoting the robot at public events; billboard, radio, and television advertisements; and prominent placement on websites — may overestimate benefits, overpromise results, and/or fail to define specific risks, leading to inflated patient perceptions.[29]

A 2011 study that examined robotic surgery information on 400 U.S. hospital websites concluded that hospital marketing of robots touted benefits, often ignored risks, and was strongly influenced by the manufacturer.

Case Example

Accurately portraying the benefits and risks of treatment is vital for patients to make informed decisions about their care. Failure to do so might result in patients feeling misled, which could potentially lead to a malpractice claim. In a recent case, for example, a doctor proposed a robot-assisted hysterectomy as an alternative treatment option for a woman who knew little about the procedure. The patient agreed to the surgery based on the doctor's recommendation and YouTube videos that extoled the precision of surgical robots. Unfortunately, during the course of the procedure, surgeons punctured the patient's bowel. The costly injury required nine operations to fix, and the patient had to be hospitalized multiple times. Following the incident, the patient stated that she felt deceived by the optimistic marketing of the robot from her doctor and the manufacturer.

Of the 41 percent of hospital websites that included robotic surgery information, 73 percent used manufacturer-provided stock images and text. Eighty-six percent made statements about the clinical superiority of robotic surgery, but few provided comparative data.[30]

Managing patients' expectations related to robotic surgery...may prove challenging for healthcare organizations and surgeons.

The study's authors explained that "Because patients regard information on hospital websites as medical opinion of the physicians working at that hospital, hospital website information carries credibility that can influence patient choice."[31]

These same concerns prompted the American Congress of Obstetricians and Gynecologists (ACOG) to release a statement addressing robotic surgery for hysterectomies. In that statement, ACOG's president stressed the necessity of providing patients with factual information and education about their treatment options.[32] The 2013 Massachusetts advisory echoed this sentiment and encouraged hospitals to pay attention to whether their marketing efforts have influenced how they select patients.[33]

A careful review of advertising and marketing efforts promoting robotic surgery may help healthcare organizations and medical staff pinpoint potentially misleading statements and identify opportunities for clarity. Ultimately, these strategies might assist patients in making more educated and informed decisions about their care.

Informed Consent

Concerns about aggressive marketing not only point to the need for accurate, objective verbal and written information, but they also highlight the essential role of informed consent in robotic surgery. Yet, because robotic surgery is fairly new, the "standard of disclosure of the risks and benefits that hospitals must provide each patient is fluid and evolving."[34]

However, many of the same considerations for informed consent that were discussed in the telehealth article in this issue of *Protector* also apply to robotic surgery. For example, in addition to standard and required consent information, each patient should be educated about:

- The procedure he or she is having and how it is performed;
- The potential risks of robotic surgery, particularly in relation to his or her specific condition;
- The surgeon's past experience with robotic surgery, particularly with the recommended robotic procedure;
- Alternative options for treatment; and
- What will happen in the event of an emergency or complication (e.g., the surgeon will switch to open surgery or traditional laparoscopy), as well as any related risks.

Taking the time to provide the patient with these details and answer any questions can help ensure that the patient has the appropriate information to make informed decisions about his or her care. As with clinical decision-making, the surgeon should document the informed consent process in the patient's medical record and include copies of any related consent forms (with patient signature).

Conclusion

The concept of robot-assisted surgery likely seemed far-fetched in the not too distant past. Today, however, the concept is a reality, and the reality is growing by leaps and bounds. Many factors have contributed to the rise of this technology, including the pursuit of new minimally invasive treatment options, strategic healthcare decisions, savvy marketing, and patient demand.

Although the possibilities and potential that robotic surgery offer are exciting, they should not overshadow patient safety and risk concerns. Hospitals, healthcare organizations, and surgeons who utilize RSS should be aware of key risk areas related to robotic surgery, such as training, credentialing, proficiency, patient selection, and informed consent.

Developing greater awareness of the risks and establishing training and credentialing guidelines, patient selection criteria, emergency protocols, detailed informed consent processes, and performance monitoring standards can help enhance safety initiatives and minimize liability exposure. ■

Questions to Consider

The healthcare community can anticipate that malpractice claims involving robotic surgery will grow as the number of robot-assisted surgeries increases each year. Although each case will be unique, some questions that might be considered as part of the discovery and litigation process include:

- What are the strengths and limitations of the surgical system used in the procedure?
- Did the patient have a preexisting condition that made him/her an undesirable candidate for robotic surgery?
- Did an informed consent process take place and was it documented?
- How many robotic surgeries has the surgeon performed?
- How often during the course of robotic surgery has the surgeon had to convert to a traditional laparoscopic procedure or open surgery?
- What are the surgeon's and/or hospital's morbidity/mortality rates for similar procedures?
- How many procedures similar to the patient's are suggested for proficiency and competency?
- How much and what types of training has each member of the surgical team received? Has the training been documented?
- Did the lead surgeon oversee or approve the surgical setup?

Source: Peters, J. D. (2012, May). Robots holding the scalpel. *Trial, 48*(5), 36–40.

Endnotes

1 Lowes, R. (2013, September 5). Complications of robotic surgery underreported, study says. Medscape. Retrieved from http://www.medscape.com/viewarticle/810490

2 Society of Gastrointestinal and Endoscopic Surgeons–Minimally Invasive Robotic Association (SAGES-MIRA) Consensus Group. (2007). A consensus document on robotic surgery. Retrieved from http://www.sages.org/publications/guidelines/consensus-document-robotic-surgery/

3 Carreyrou, J. (2010, May 4). Surgical robot examined in injuries. *The Wall Street Journal.* Retrieved from http://online.wsj.com/news/articles/SB10001424052702304703104575173952145907526

4 Bhavna, J. K., Dodwad, V., & Singh, T. (2012). Robotic dentistry — The future is at the horizon. *Journal of Pharmaceutical and Biomedical Sciences, 16*(16).

5 Sindet-Pedersen, S. (2013, February). The use of robotics in dentistry. *Today International AEEDC Dubai 2013*, p. 6.

6 Peters, J. D. (2012, May). Robots holding the scalpel. *Trial, 48*(5), 36–40.

7 Sullivan, M. J., Frost, E. A. M., & Lew, M. W. (2008). Anesthetic care of the patient for robotic surgery. *Middle East Journal of Anesthesiology, 19*(5), 967–982.

8 Commonwealth of Massachusetts Board of Registration in Medicine. (2013, March). Advisory on robot-assisted surgery. Retrieved from http://www.mass.gov/eohhs/docs/borim/physicians/pca-notifications/robot-assisted-surgery.pdf

9 Langreth, R. (2013, November 11). Robot surgical incidents may pressure hospital training. Bloomberg. Retrieved from http://www.bloomberg.com/news/2013-11-11/robot-surgery-incidents-may-pressure-hospital-training.html

10 Lowes, R. (2013, April 30). FDA investigates robotic surgery system after adverse even spike. Medscape. Retrieved from http://www.medscape.com/viewarticle/803339

11 Intuitive Surgical. (2013). Investor presentation: Q4 2013. Retrieved from http://www.intuitivesurgical.com/

12 Kowalczyk, L. (2013, March 26). Mass. cautions hospitals about robotic surgery. *The Boston Globe.* Retrieved from http://www.bostonglobe.com/lifestyle/health-wellness/2013/03/25/state-cautions-hospitals-about-patient-complications-during-robot-assisted-surgery/xOAsxR80qH5mVENDdktjKL/story.html

13 ECRI Institute. (2012). Top 10 C-Suite watch list: Hospital technology issues for 2012, 12–14.

14 ECRI Institute. (2013). Top 10 health technology hazards for 2014. Retrieved from https://www.ecri.org/2014hazards

15 Langreth, R. (2013, March 21). Intuitive robosurgery training seen lacking in lawsuits. Bloomberg. Retrieved from http://www.bloomberg.com/news/2013-03-21/intuitive-robosurgery-training-seen-lacking-in-lawsuits.html; Ostrom, C. M. (2013, May 3). Failed robotic surgery focus of Kitsap trial. *The Seattle Times.* Retrieved from http://seattletimes.com/html/localnews/2020918732_robottrialxml.html

16 Ibid; Peters, Robots holding the scalpel; ECRI Institute, Top 10 health technology hazards for 2014.

17 Liberman, D., Trihn, Q. D., Jeldres, C. Valiquette, L., & Zorn, K. C. (2011). Training and outcome monitoring in robotic urologic surgery. *Nature Reviews Urology, 9*(1), 17–22; Lee, J. Y., Mucksavage, P., Sundaram, C. P., & McDougall, E. M. (2011, April). Best practices for robotic surgery training and credentialing. *The Journal of Urology, 185*, 1191–1197; Schreuder, H. W. R., Wolswijk, R., Zweemer, R. P., Schijven, M. P., & Verheijen, R. H. M. (2012). Training and learning robotic surgery, time for a more structured approach: A systematic review. *BJOG, 119*, 137–149.

18 SAGES-MIRA, A consensus document on robotic surgery.

19 Ibid.

20 Aston, G. (2012, April). Surgical robots worth the investment? Hospitals and Health Networks. Retrieved from http://www.hhnmag.com/display/HHN-news-article.dhtml?dcrPath=/templatedata/HF_Common/NewsArticle/data/HHN/Magazine/2012/Apr/0412HHN_FEA_clinicalmanagement

21 Peters, Robots holding the scalpel.

22 U.S. Food and Drug Administration (FDA), Medical Product Safety Network. (2013, November). Small sample survey — final report. Retrieved from http://www.fda.gov/downloads/medicaldevices/productsandmedicalprocedures/surgeryandlifesupport/computerassistedroboticsurgicalsystems/ucm374095.pdf

23 Peters, Robots holding the scalpel; Langreth, Intuitive robosurgery training seen lacking in lawsuits.

24 Sullivan, et al., Anesthetic care of the patient for robotic surgery; Kowalczyk, Mass. cautions hospitals about robotic surgery.

25 Ostrom, Failed robotic surgery focus of Kitsap trial.

26 FDA, Small sample survey.

27 Commonwealth of Massachusetts Board of Registration in Medicine, Advisory on robot-assisted surgery.

28 Clark, C. (2012, April 17). Da Vinci robot surgical risks detailed. HealthLeaders Media. Retrieved from http://www.healthleadersmedia.com/page-1/TEC-279018/Da-Vinci-Robot-Surgical-Risks-Detailed

29 Langreth, R. (2013, October 8). Robot surgery damaging patients rises with marketing. Bloomberg News. Retrieved from http://www.bloomberg.com/news/2013-10-08/robot-surgery-damaging-patients-rises-with-marketing.html

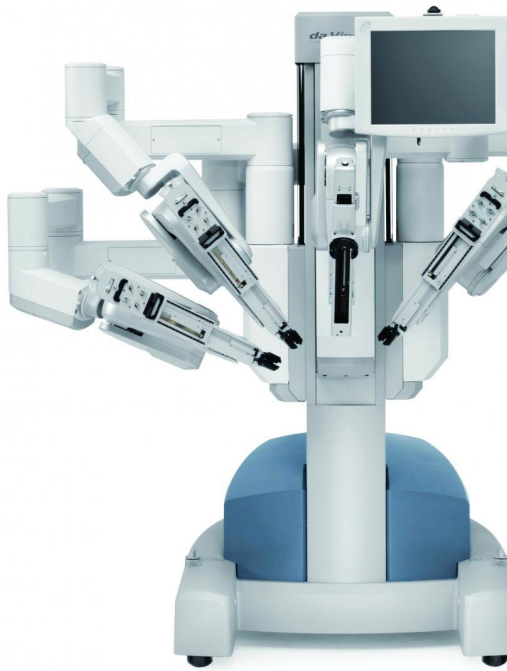
30 Jin, L. X., Ibrahim, A. M., Newman, N. A., Makarov, D. V., Pronovast, P. J., & Makary, M. A. (2011). Robotic surgery claims on United States hospital websites. *Journal for Healthcare Quality, 33*(6), 48–52.

31 Ibid.

32 The American Congress of Obstetricians and Gynecologists (ACOG). (2013, March 14). Statement on robotic surgery by ACOG President James T. Breeden, MD. Retrieved from https://www.acog.org/About_ACOG/News_Room/News_Releases/2013/Statement_on_Robotic_Surgery

33 Commonwealth of Massachusetts Board of Registration in Medicine, Advisory on robot-assisted surgery.

34 Peters, Robots holding the scalpel.



Keeping a Finger on the Pulse of Social Media in Healthcare: Understanding Evolving Roles and Risks

Viviane Jesequel

Viviane Jesequel, RN, BS, HCRM

"Social media" is simply a broad umbrella term that covers a wide range of electronic communication tools, such as email, social networking websites, blogs, video sharing and conferencing tools, mobile applications, and more.

The growth and usage of social media continue to influence not only the American public, but the world at large. Estimates suggest that nearly 1 in 4 people use social networks.[1] With the rapid expansion of these technologies, one can assume that in 2014 and beyond, social media will become even more prevalent.

In the past, healthcare was relatively slow to implement social media tools, primarily because of concerns regarding the potential risks of violating patient privacy. However, over the past few years, an increase in implementation has occurred — mainly due to consumer demand.

A 2013 article from *Healthcare IT News* says "It's no secret that a growing percentage of today's patients are increasingly using digital tools as part of their overall health maintenance. In fact, a recent Pew Research Center study said that 1 in 3 American adults have used the web to figure out a medical issue. In another survey . . . 41% of people said social media would affect their choice of healthcare provider."[2]

With this growing emphasis on electronic communication and the importance that patients place on it, physicians and dentists might be eager to implement these technologies in their practices. However, leveraging social media for professional purposes can be a slippery slope, and its usage in healthcare presents various challenges.

This article discusses common risk concerns associated with using social media for healthcare communication and delivery, and it offers risk-reduction strategies that doctors and their staffs can implement.

Leveraging social media for professional purposes can be a slippery slope, and its usage in healthcare presents various challenges.

What Are the Potential Benefits of Social Media?

The use of social media can bring significant communication and educational benefits to both healthcare providers and consumers.

A 2010 Google study indicated that 86 percent of American physicians use the Internet to gather health and medical information.[3] Many doctors use social media to stay up to date with new information that may affect their practices and patient care. Further, social media is used as an online marketing tool to increase provider visibility and reputation, as well as enhance professional networking.

For consumers, social media can assist them in searching for a new physician or dentist, keeping up with healthcare issues and concerns, finding support groups, researching alternative medications and side effects, and more.

What Types of Social Media Tools Are Available?

A myriad of social media applications and tools are available. Some common ones that are used for both personal and professional purposes include:

- **Email.** Email is a very commonly used and recognized form of social media, and it has become an increasingly viable communication option for healthcare providers and patients. Patients may use emails to ask questions, request medication refills, report symptoms, schedule appointments, and more.
- **Facebook.** With more than 1 billion active users per month, Facebook allows users to share information, pictures, and videos; follow individuals, organizations, and groups; converse via electronic messaging; and more. The site allows for both personal and professional pages.

The Big Picture

Social media has experienced an explosion in popular culture. Did you know that:

- Facebook has more than 1 billion active monthly users and 665 million daily users?
- Twitter has approximately 500 million tweets per day?
- YouTube has more than 1 billion unique monthly visitors. More than 6 billion hours of video are watched each month, and about 100 hours of video are uploaded every minute?
- LinkedIn has 250 million members in over 200 countries and territories around the globe.

Sources:
https://www.facebook.com/facebook
https://about.twitter.com/company
http://www.youtube.com/yt/press
http://www.linkedin.com/about-us

- **LinkedIn.** LinkedIn focuses on professional relationships and includes job-related information, access to recruiters, professional networking opportunities, and career-related articles and topics.
- **Twitter.** Twitter is a microblogging site that promotes real-time sharing of information and up-to-the minute news from individuals or organizations.
- **Skype and FaceTime.** Skype and FaceTime are both video-chatting technologies that allow users to interact in real-time over an Internet connection.
- **YouTube.** YouTube is a video-sharing site that allows user to upload, view, and share videos on a wide range of topics for both entertainment and educational purposes.
- **Patient portals.** Patient portals, which are a relatively new technology, allow patients to access their health records and communicate with their healthcare providers through a secure online website.

Deciding which applications and tools will be most helpful will largely depend on the context and needs of your practice. However, when determining how to use these technologies to communicate with patients, carefully consider the goal of the communication, the target audience, and what types of information you plan to promote (e.g., advertisements, health education, etc.).

What Are the Risks of, and Strategies for, Using Social Media?

Undoubtedly, social media offers various functions that may potentially enhance the dissemination of healthcare information and communication between patients and providers.

But what about the risks? Like any type of technology, social media can create safety and liability issues if it is not used responsibly. Additionally, because the social media landscape is rapidly changing, standards and best practices are not always well-defined.

Like any type of technology, social media can create safety and liability issues if it is not used responsibly.

To address these challenges, healthcare providers should be aware of the potential risks associated with electronic communication, develop detailed social media policies, and implement risk strategies to safeguard their patients and practices.

Maintain Privacy and Security

One of the most significant concerns related to social media is the requirement to maintain strict confidentiality and safeguard patients' protected health information (PHI). This obligation is addressed in federal law and governed by the U.S. Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Individual states also may have laws related to privacy and security of PHI, which might be more stringent than federal laws.

Because the boundaries between appropriate vs. inappropriate and personal vs. professional use of social media can easily blur, managing privacy risks can be challenging. For example, numerous instances have occurred in which healthcare workers have posted pictures of, or details about, their patients on their professional or personal social media pages without the patients' consent. Regardless of whether these actions were intentional or inadvertent, they violated confidentiality and the patients' privacy rights.[5]

A number of risk strategies can help practices address privacy concerns related to social media. For example:

- Do no post or publish any content on social media sites that contains patient details or identifying information (including photographs and testimonials), without the patient's permission and written consent. The consent should explicitly state how the information will be used.
- Consider prohibiting the photographic use of cell phones and other mobile technologies as part of office policy.
- Have someone who is familiar with HIPAA and state privacy regulations review social media content to ensure information does not violate patient confidentiality.
- Train staff on HIPAA and state privacy laws, and educate them about the consequences of violating these regulations.

Because the boundaries between appropriate vs. inappropriate...use of social media can easily blur, managing privacy risks can be challenging.

> "Social media may make privacy violations more concerning than they might otherwise be because they distribute information instantaneously to a wide audience and because, unlike verbal conversations, use of social media creates a permanent electronic record that is likely discoverable in litigation."[4]

- Ask staff members to sign confidentiality agreements, and maintain a signed copy of the agreement in each employee's personnel file.
- Be aware that responding to a patient post or review on a social media site might violate privacy laws.
- Understand the technical limitations and terms and conditions of any social media sites that you plan to use. For example, information sent via messaging functions is likely not encrypted, and the site may maintain the right to access any personal information.

Addressing privacy concerns in your practice's social media policies and implementing strategic safeguards can help protect patients and reduce liability exposure.

Establish Appropriate Boundaries

Social media can create a new dynamic in, and pose new challenges related to, the doctor–patient relationship. In April 2013, the American College of Physicians

(ACP) and the Federation of State Medical Boards (FSMB) released a position paper titled *Online Medical Professionalism: Patient and Public Relationships: Policy Statement*, which explained that "Use of online media can bring significant educational benefits to patients and physicians, but may also pose ethical challenges."[6]

In speaking with *HealthLeaders Media*, Dr. Humayun Chaudhry, FSMB President and CEO, warned that "Anything physicians post on sites can be forwarded, taken out of context, and accessed and retrieved in perpetuity. That's a fact that many physicians don't always think about when they engage in social media."[7]

Because social media is used for both personal and professional purposes, the boundaries between the two can sometimes become difficult to distinguish. However, healthcare providers can generally make two assumptions: (1) any of their staff members or patients could be using some type of social media, and (2) anyone could potentially read what they and/or their staff members post, as well as what anyone else writes about their practice or organization on social media sites.[8]

Because of these concerns about personal and professional boundaries, the ACP-FSMB paper advises doctors to keep their personal and professional social media activities separate and to "comport themselves professionally in both."[9]

For example, doctors should not "friend" patients on Facebook or mix social relationships with their professional relationships. Instead, they should apply the same ethical principles that govern their traditional patient encounters to their online interactions with patients, including privacy and confidentiality standards.

Further, doctors should be aware of the implications of providing online information that might be construed as medical or dental advice. Doing so could inadvertently trigger a duty to care, and it may also pose patient safety concerns. Because of this, electronic media should include standard disclaimers and disclosure language that explain the nature of the communication (e.g., for informational purposes only) and caution users against interpreting the materials as medical or dental advice.

[Doctors] should apply the same ethical principles that govern their traditional patient encounters to their online interactions with patients.

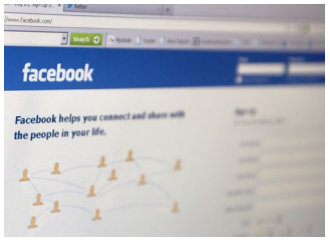
Develop Social Media Policies

The development and implementation of social media policies and guidelines is essential to managing risks associated with these technologies. Include staff in the initial planning and drafting of policies, and ask them to help identify and assess potential issues.

Key areas to consider when developing your practice's social media policies include:

- The practice's goals and target audience for social media communication;
- Acceptable and unacceptable use of social media, with explicit examples;
- Who is authorized to develop and post social media content on behalf of the practice;
- The review and approval process for social media content;
- Standard disclaimer and disclosure language;
- The patient consent process;
- Terms of use for users on your sites; and
- The process for reporting inappropriate use of social media.

When developing these policies, keep in mind that social media is dynamic and constantly changing. To address this, create policies that are flexible and adaptable to new or changing social media technologies. Doing so will help avoid the need for constant updating.[10]



Email policies. In addition to having policies for social media websites (such as Facebook and Twitter), practices also should have written guidelines for the use of email and other types of electronic messaging.

The American Medical Association (AMA) realized years ago that email would be a valuable communication tool in healthcare. As such, they developed guidelines for the ethical use of email between doctors and patients. Although the guidelines noted many beneficial aspects of email communication, they also outline four key precautions to help manage risks.

1. Email should not be used to establish a doctor–patient relationship; rather, it should be used to supplement traditional patient encounters.
2. The same ethical responsibilities that apply to in-person patient encounters also apply to email communication.
3. Doctors should properly notify patients of the limitations of email communication, such as delays in response and potential security issues.
4. Doctors should provide proper notification of email's limitations prior to initiating email correspondence or in the initial email communication.[11]

The American Dental Association (ADA) reiterated these concerns in a 2007 publication, noting that although email communication in the dental office can be very beneficial, it can also "raise significant considerations." Like the AMA, the ADA cautions that patients should be notified about, and accept the risks of, communicating via email before such communication is used.[12]

When developing an email consent form, medical and dental practices may want to consider including the following types of information:

- Type of communication permitted (i.e., for what purpose(s) will the practice use email?);
- Criteria for establishing the patient relationship;
- Notice of whether the office email is encrypted;

- A statement notifying patients to contact 911 if they are experiencing an urgent problem;
- The general turnaround time for responding to email; and
- The right of the physician to refuse to make conclusions or decisions regarding treatment based on information obtained online.

The email consent form should also include (a) a statement that the patient has read and accepted the policy, and (b) a place for the patient's signature. The practice should maintain the signed release in the patient's record.

Control Quality and Monitor Your Online Presence

Part of maintaining a professional presence online is monitoring the quality of information posted or sent on behalf of your practice. Information should be accurate, current, objective, and nonambiguous. Policies that establish who is responsible for developing content and how content is reviewed and approved will assist with quality control efforts.

Understanding the types of media your practice is using and how users can potentially interface with it are important aspects of quality control.

Depending on the type of social media being used and/or the control settings, site users might be able to post content or comments to your practice's social media pages. Understanding the types of media your practice is using and how users can potentially interface with it are important aspects of quality control.

As part of social media policies, medical and dental practices should include a mechanism for monitoring their online presence and responding to negative, offensive, or inaccurate information. To ensure consistency with organizational policy, practices might want to consider assigning one person to review external comments, posts, responses, etc. and respond accordingly. Keep in mind that comments and responses from practice staff must comply with privacy standards.

Educate Staff

When integrating social media into your practice's communication initiatives, it is important to educate staff about how much and what types of personal and professional social media usage and tools are acceptable in the practice.

A recent survey found that 75 percent of employees were accessing their personal social media sites from their mobile devices at least once a day and 60 percent were accessing these sites multiple times throughout the day.[13]

A significant challenge in the office practice setting is instilling common sense and discretion regarding the use of social media for both personal and professional purposes. Practice policy should define appropriate use of the Internet and mobile devices (such as tablets and cell phones). For example, the policy might require that employees turn off their personal phones during office hours and retrieve and respond to their messages during breaks or at lunch time.

Education about the practice's social media policies, as well as discussions about the potential risks and liability issues associated with social media, should be included as part of orientation training and ongoing staff education. Staff members also should be aware of the disciplinary actions for violating the social media policy.

Conclusion

In the years ahead, as the role of social media continues to evolve, it will be essential for medical and dental practices to ensure a safe and effective environment for patients, staff, and providers to communicate electronically.

Given the number of options available for electronic communication and networking, careful consideration must be given to choosing the appropriate format that meets the needs of your practice and patient population.

Further, maintaining privacy and confidentiality, establishing appropriate boundaries, developing written policies, monitoring online presence, and educating staff should always remain in the forefront of utilizing social media in healthcare. ■

Viviane Jesequel is a senior risk management consultant at Medical Protective. She has more than 25 years of experience in the healthcare industry and has achieved an understanding of the challenges and opportunities facing both clinicians and hospitals. Viviane's expertise includes consulting with clients regarding patient safety and quality/performance improvement, identifying and evaluating potential liability exposures, and developing solutions to reduce or eliminate loss severity.

Endnotes

1 Taylor, K. (2013, October 11). Where social-media use is growing the most. *Entrepreneur.* Retrieved from http://www.entrepreneur.com/article/228734#

2 Trader, J. (2013, June 24). Social media and healthcare: Navigating the new communications landscape. Retrieved from http://www.healthcareitnews.com/blog/social-media-and-healthcare-navigating-new-communications-landscape

3 Council on Ethical and Judicial Affairs. (2010). Professionalism in the use of social media (CEJA Report 8-I-10). American Medical Association. Retrieved from http://www.ama-assn.org/resources/doc/code-medical-ethics/9124a.pdf

4 ECRI Institute. (2011, November). Social media in healthcare. *Healthcare Risk Control, Supplement A.*

5 Ibid.

6 Farnan, J. M., Sulmasy, L. S., Worster, B. K., Chaudhry, H. J., Rhyne, J. A., & Arora, V. M. (2013). Online medical professionalism: Patient and public relationships: Policy statement from the American College of Physicians and the Federation of State Medical Boards. *Annals of Internal Medicine, 158*(8), 620–627.

7 Clark, C. (2013, April 12). ACP, FSMB issue stern guidance on social media. Retrieved from http://www.healthleadersmedia.com/print/PHY-291079/ACP-FSMB-Issue-Stern-Guidance

8 The Medical Protective Company. (2011). *Social media guideline.* Fort Wayne, IN: Medical Protective.

9 Farnan, et al., Online medical professionalism.

10 ECRI Institute, Social media in healthcare.

11 American Medical Association. (2003, June). Opinion 5.026 — the use of electronic mail. Retrieved from http://www.ama-assn.org//ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5026.page

12 American Dental Association. (2007). Dental records. Retrieved from http://www.raedentalmanagement.com/pdfs/ADA_Dental_Records.pdf

13 SilkRoad. (2012). Social media and workplace collaboration report: 2012 latest practices, key findings, hottest topics. Retrieved from http://www.silkroad.com/Resources/eBooks/2012/10/Social_Media_and_Workplace_Collaboration_Report.html

Social Media Checklist

Whether your practice is already using social media or planning to implement a social media strategy, this checklist can help you focus on some key risk management considerations. For more detailed information or specific concerns related to social media, contact your risk management consultant at 800–4MEDPRO.

	YES	NO
Has your practice considered its social media strategy, including the goal of the communication, the target audience, and what types of information will be promoted?	☐	☐
Does your practice have an approved policy or set of policies on the use of social media, including email? If not, is one in development?	☐	☐
If your practice does have a social media policy, do staff and healthcare providers understand the policy?	☐	☐
Does your social media policy specifically state who is authorized to develop content, and does it outline a detailed plan for content review and approval?	☐	☐
Does your practice provide training on social media policies as part of new employee orientation and ongoing staff education?	☐	☐
Have staff members received HIPAA training, and are they aware of their obligation to maintain patient privacy? Have they signed confidentiality agreements?	☐	☐
Does your practice's social media policy include disciplinary actions for policy violations? Are consequences consistent with existing patient privacy and confidentiality policies?	☐	☐
Are staff members aware of how to report inappropriate use of social media?	☐	☐
Does your practice have a mechanism to monitor social networking sites for negative comments (including comments about adverse events) by consumers, patients, and employees? If so, does your policy include how to respond to such comments?	☐	☐
Do existing information technology (IT) security policies and procedures take into account social media?	☐	☐
Does your practice include standard disclaimers and disclosure statements with each electronic interaction?	☐	☐
Has your practice incorporated the use of social media by all levels of staff and providers into your annual risk assessment?	☐	☐

Medical Protective
a Berkshire Hathaway company
Strength. Defense. Solutions. Since 1899.

To sign up to receive future issues of *Protector* electronically, visit www.medpro.com/protector.

PRSRT STD
U.S. POSTAGE
PAID
MILWAUKEE, WI
PERMIT NO. 4550

5814 Reed Road
Fort Wayne, IN 46835-3568

Visit us at medpro.com or call 800-4MEDPRO.