HEALTHCARE RISK MANAGEMENT™

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

INSIDE

RELIAS MEDIA

MARCH 2019 Vol. 41, No. 3; p. 25-36

Evolution of Healthcare Industry Poses New and Ongoing Compliance Risks in 2019

Legal experts focusing on healthcare compliance say there will be plenty to keep healthcare risk managers busy in the coming months, with more emphasis on telemedicine, electronic health records (EHRs), and opioids. The continuing move to value-based care also is creating new challenges for compliance with laws that were designed in a fee-for-service era.

The challenges in healthcare compliance continue to expand, says **Anjali N.C. Downs**, JD, an attorney with the Epstein Becker Green law firm in Washington, DC. Healthcare entities must focus on cybersecurity to ensure that they have robust systems in place to protect the privacy and security of patient and consumer data, she says.

> HEALTHCARE ENTITIES NEED TO REMAIN VIGILANT IN STAYING ON TOP OF CHANGING REGULATIONS AND ANALYZING HOW THOSE CHANGES MAY IMPACT OPERATIONS AND COMPLIANCE ACTIVITIES.

"In addition, EHR compliance will remain front and center. Medicare providers must meet the interoperability requirements, and in light of recent settlements, ensure that their EHR technologies are compliant. Fraud and abuse enforcement with an emphasis on criminal enforcement will continue to expand, as will an emphasis on individual liability in civil corporate investigations," Downs says. "The opioid crisis will continue to receive government

Financial Disclosure: Author **Greg Freeman**, Editor **Jill Drachenberg**, Editor **Jesse Saffron**, Editorial Group Manager **Terrey L. Hatcher,** and Nurse Planner **Maureen Archambault** report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study. Consulting Editor **Arnold Mackles**, MD, MBA, LHRM, discloses that he is an author and advisory board member for The Sullivan Group and that he is owner, stockholder, presenter, author, and consultant for Innovative Healthcare Compliance Group.

HEALTHCARE RISK MANAGEMENT™

***Healthcare Risk Management™*, ISSN 1081-6534, *including Legal Review & Commentary*,™ is published monthly by Relias LLC, 1010 Sync St., Ste. 100, Morrisville, NC 27560-5468. Periodicals postage paid at Morrisville, NC, and additional mailing offices. POSTMASTER: Send address changes to *Healthcare Risk Management*, Relias LLC, 1010 Sync St., Ste. 100, Morrisville, NC 27560-5468.**
GST Registration Number: R128870672

SUBSCRIBER INFORMATION: Customer Service: (800) 688-2421. ReliasMediaSupport@reliasmedia.com ReliasMedia.com

SUBSCRIPTION PRICES: USA, Print: 1 year (12 issues) with free CE nursing contact hours, $519. Add $19.99 for shipping & handling. Online only, single user: 1 year with free CE nursing contact hours, $469. Outside USA, add $30 per year, total prepaid in USA funds.

MULTIPLE COPIES: Discounts are available for group subscriptions, multiple copies, site licenses, or electronic distribution. For pricing information, please contact our Group Account Managers at groups@reliasmedia.com or (866) 213-0844. Missing issues will be fulfilled by customer service free of charge when contacted within one month of the missing issue date. Back issues, when available, are $87 each.

ACCREDITATION: Relias LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation. Contact hours [1.5] will be awarded to participants who meet the criteria for successful completion. California Board of Registered Nursing, Provider CEP#13791.

Relias LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians. Relias Learning designates this enduring material for a maximum of 1.5 *AMA PRA Category 1 Credits™*. Physicians should claim only credit commensurate with the extent of their participation in an activity.

Healthcare Risk Management™ is intended for risk managers, healthcare administrators, healthcare legal counsel, and physicians.

This activity is valid 36 months from the date of publication.

Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

AUTHOR: Greg Freeman
EDITOR: Jill Drachenberg
EDITOR: Jesse Saffron
EDITORIAL GROUP MANAGER: Terrey L. Hatcher
SENIOR ACCREDITATIONS OFFICER: Lee Landenberger

EDITORIAL QUESTIONS
Call Editor **Jill Drachenberg**, (404) 262-5508

attention, and fraud enforcement in the opioid context is likely to expand beyond just federal healthcare payers."

Downs says she is hopeful that 2019 will bring new Stark Law and Anti-Kickback regulations focused on easing the regulatory burdens and promoting value-based payment methodologies. Until then, healthcare entities wanting to focus on care coordination and value-based systems must continue to navigate the rigidness of fraud and abuse laws that were designed for fee-for-service payment methodologies.

"Expect regulatory reforms that are focused on drug rebates. The Office of the Inspector General of HHS issued a proposed rule restricting Anti-Kickback safe harbor protection for pharmaceutical rebates from manufacturers to Part D plan sponsors, Medicaid managed care organizations, and contracted PBMs [pharmacy benefit managers], while expanding protection for point of sale rebates that meet specific elements of the safe harbor," Downs notes.

"If adopted, the proposed rule would go into effect Jan. 1, 2020, so those impacted by the proposed rule must watch developments to ensure that they have made any necessary adjustments or restructuring."

In addition to the Anti-Kickback Statute, which will continue to play a role in fraud enforcement in the opioid crisis, the Eliminating Kickbacks in Recovery Act of 2018 (EKRA) contains specific criminal provisions to prevent fraud and kickbacks for referrals for substance abuse treatment payable by federal healthcare programs and commercial payers, Downs notes. EKRA appears to have a broad reach, potentially implicating all arrangements for laboratory services, she says.

"Likewise, as evidenced through the DOJ's actions in seeking a permanent injunction against prescribing and practicing medicine of two physicians in Ohio, federal and state governments will continue to aggressively pursue fraudulent schemes in which providers write illegal prescriptions or submit claims to Medicare, Medicaid, TRICARE, and private insurance companies for treatments that were medically unnecessary," Downs says.

Healthcare entities need to remain vigilant in staying on top of changing regulations and analyzing how those changes may impact operations and compliance activities, she says.

To address cybersecurity concerns, organizations should assess current practices and consider having a formal risk assessment and review of current cybersecurity infrastructure.

Regarding the opioid crisis, organizations should review and audit physician prescription practices, marketing activities, and relationships with vendors and

EXECUTIVE SUMMARY

The changing face of American healthcare is bringing new challenges for regulatory compliance. Value-based care is clashing with laws that were written to discourage fee-for-service fraud.

- Cybersecurity continues to create liability risks in healthcare.
- Licensing requirements are holding back the advance of telemedicine.
- Data analytics could help reduce liability risks.

substance abuse treatment facilities, she suggests.

Physicians Must Justify Decisions

For physicians, thorough documentation and justification of medical decisions is the key to compliance, says **Brad Fell**, MD, head of compliance for Allied Physicians Group, a pediatric group with 32 offices, 150 doctors, and more than 400 staff members operating in New York City.

Insurance carriers are constantly looking to take back money and require more and more prior authorizations to provide the proper care to patients, he notes. In addition, the patients are paying significantly higher insurance premiums but are receiving fewer fully covered services.

Patient responsibilities, including higher copays, deductibles, and noncovered or partially covered services, are damaging the patient-doctor relationship, he says.

"This could even prevent physicians from providing the proper standard of care as many patients refuse common services because they know their carrier is going to make it the patient's responsibility to pay," Fell says. "Then the physician is put in the ethical, moral, and compliance issue of providing the service and waive the fee — which is a compliance issue — or allow the patient to refuse, knowing their care is now substandard."

The new tax implication for waiving or writing off patient payments has begun to affect hospitals and very large corporations in the past two years, Fell notes. The total expected taxable revenue will be the amount that was supposed to be collected, not the amount actually collected, he explains. That has led some organizations to forbid waiving fees.

Fell emphasizes the importance of establishing a comprehensive compliance program.

"[Perform] yearly audits on all providers to review if documentation is supporting the services billed out. Evaluate procedure productivity reports to make sure providers aren't overperforming services unnecessarily. Provide corrective action plans for providers that your compliance plan has concerns about," he says. "Provide yearly education to all staff and providers. Have regular compliance meetings with updates regarding new rules and regulations, as well as sending out education updates to the staff and providers."

More Documentation at Encounter

Healthcare compliance is ever increasing, with several specific hot areas being risk adjustment, data security, quality reporting, Medicare Access and CHIP Reauthorization Act/Merit-Based Incentive Payment System (MACRA/MIPS), and changes to the Medicare Shared Savings Program, says **Michael Meng**, chief financial officer at Stellar Health, a technology services company in New York City that assists healthcare organizations with value-based care.

"In risk adjustment, there is an increased focus to push the completion of proper documentation and coding closer to the providers that are responsible for providing care to the patient. Historically, CMS has allowed end-of-year, retrospective RAPS [Risk Adjustment Processing System] submissions for risk adjustment, but increasingly we will see this moved toward the encounter, when the provider is treating the patient," Meng explains. "This means it will be even more important for health insurers to work with providers to get them to carry out this documentation at the frontlines of care."

In the transition to value-based care thus far, most of the solutions have focused on and ended at the contracting entity, Meng says. But to effectuate change, payers need to deliver value-based care to that last mile of workflow: the doctors and office support staff.

Meng says another major challenge and regulatory change in healthcare is the CMS Final Rule issued on Dec. 21, 2018, regarding the Medicare Shared Savings Program. This new rule sunsets the ability for accountable care organizations (ACOs) to remain upside-only and pushes them toward taking on two-sided risk much sooner than originally planned.

"While at first glance this seems to only impact ACOs and push them toward risk, most providers in this country have joined such ACOs, as they either have to take risk with MACRA/MIPS reporting or be part of a Medicare ACO," Meng says. "This final rule essentially pushes all providers in this country toward either taking on MACRA/MIPS with rewards and penalty components or being part of an ACO program that also has both upside and downside risk to it."

Value-Based Care Instituted Unevenly

The move toward value-based care is unevenly distributed, notes **Michael B. Lampert**, JD, partner with the Ropes & Gray law firm in

Boston. In some areas, it is relatively mature; in many others, it is nascent or even still on the horizon, he says.

"But it has led to changes across the industry, as any change in reimbursement models would be expected to do. Reimbursement is money; money motivates, and the healthcare industry is no exception," Lampert says. "New reimbursement models naturally, and by their very design, affect the behavior of payers, providers, suppliers, manufacturers, and patients. They create new incentives, call for new affiliations, put attention to new measures, and, as a result of all of that, create a new legal and regulatory risk environment."

Lampert says there are three commonalities in value-based reimbursement arrangements that contribute to their presentation of new compliance risks. First, value-based reimbursement models intend to use financial incentives to change behavior in healthcare management and delivery. But many laws have developed over the decades specifically to keep financial considerations out of the picture. The collision of approaches inherently creates questions of compliance, he says.

Second, value-based reimbursement models seek to integrate health management and care delivery, calling on participants in the system to collaborate with others outside of their own organization and to find new ways of interacting with patients, sometimes more affirmatively.

"Cross-organizational coordination and patient engagement by its nature calls for different sorts of relationships amongst providers and payers and suppliers and others, and with patients, which present new questions of compliance, particularly with laws that were drafted anticipating a less connected environment," Lampert says.

Third, value-based reimbursement models, by paying to a lesser or greater degree on value rather than on other metrics, obviously rely on value metrics when determining what payments to make.

"From a compliance perspective, however, the significance is that the accuracy of new kinds of information matters for payment purposes, and errors with respect to that information, which previously may have mattered only for an organization's internal purposes — if at all — may carry both revenue exposure and compliance risk," he says.

Conflicts With Old Laws

The issue for healthcare organizations is not so much the changes in regulation but the lack of change, or unevenness of change, Lampert says.

"Existing regulation in many ways aims at risks presented by prior business models and reimbursement models. But the change in incentives brought by a change of reimbursement makes many of those risks less important," Lampert says. "The problem, however, isn't that those elements of existing regulation have become irrelevant. They still apply, and they still constrain conduct, but changes in the reimbursement landscape have in many areas caused that conduct not to become as worrisome as it once was, and indeed in [some] areas to become desirable."

Lampert offers the example of patient engagement. A variety of laws envision a medical system that in its ideal is almost passive, he says. A patient has a medical concern, engages with a physician, who might pass the patient along to a specialist, and the patient receives care. The process ends there.

"Envisioning that process flow, laws became anxious with provider-driven activity and engagements with patients that could interfere, increasing fees for the physician and exposing the patient to unnecessary services," Lampert explains. "Now envision a model in which physicians are responsible for keeping a population healthy for the lowest aggregate spend. Those physicians are driven, by the reimbursement model, to engage with patients who might not be adhering to care plans, or even who might not be engaging at all with the medical community but might be leading unhealthy lives."

"The engagement might be as basic as helping patients to engage in healthier living, which would include few professional fees at all," he adds. "But providers remain hesitant to do so because the laws haven't yet caught up."

Lawmakers are catching up with some of these industry evolutions, but the legal changes are unevenly dispersed, Lampert says. While Medicare Advantage plans may feel more flexibility to engage with their members around health more generally, healthcare providers have yet seen little official change.

"It has been quipped that the future is here, but simply isn't dispersed very evenly," Lampert says. "That applies in healthcare regulation, and is a source of struggle for healthcare organizations seeking to engage effectively in the market."

The most likely compliance challenge for organizations will be figuring out how to operate effectively in a reimbursement and legal environment that is in flux,

Lampert says. Many organizations are developing reasoned approaches toward engaging in areas of subjectivity where they would not have dreamed to tread 10 years ago, he says.

Some are more reticent, in some cases because of organizational temperament, and in other cases because of the current inflection point in the organization's business. For example, a company nearing a major transaction might fear that its prospective partners would find a new practice to be intolerably novel, Lampert explains.

"Overall, the biggest challenge for particularly innovating organizations will be figuring out where the lines lie. It is not a profound recipe, but the best strategies for organizations assessing how to position themselves are to assess first whether areas where they are being challenged to go are areas of legitimate benefit to patients and to the financing system, and therefore areas that ought generally to be supported," Lampert says.

"They also should see whether there are partnerships or similar structures that can reframe a new proposal into something that may be better recognized from a regulatory perspective, and thus better grounded in a turbulent time. Look to see if there are pockets of regulatory change on whose coattails the organization might fairly hitch a ride."

Telemedicine Laws Lag Behind Technology

The biggest challenges in healthcare are driven by the need to reduce costs, says **Ron Lebow**, JD, senior counsel in the Health Law Group with the Greenspoon Marder law firm in New York City. This means better care coordination and an increased focus on proactive consumer involvement through the internet, mobile apps, and other communication technologies.

However, telemedicine laws are still in the Stone Age, Lebow says, making it difficult for physicians with the appropriate expertise to coordinate care across state lines.

Physicians generally have to be licensed in each state in which the patient resides, Lebow says. This creates difficulty for telemedicine platforms — including those operated by providers and insurance companies — to implement internet or app-based solutions that draw users from across the country.

> THE MOST LIKELY COMPLIANCE CHALLENGE FOR ORGANIZATIONS WILL BE FIGURING OUT HOW TO OPERATE EFFECTIVELY IN A REIMBURSEMENT AND LEGAL ENVIRONMENT THAT IS IN FLUX.

The laws permitting cross-state care have not caught up and not all states offer licensing reciprocity. These laws and implementation through regulation are nevertheless developing at a slow place, he says.

"Currently, they provide limited exceptions to in-state licensure for consultations directly with physicians in other states and increasing exceptions for hospital-to-hospital consultations, chronic care management for certain conditions that cost the system the most, and for care for developmental disabilities," Lebow says "To complicate matters, even new mandates under the law for Medicare and insurance carriers to reimburse for certain telemedicine consultations provide room for insurers to limit reimbursement for these services depending on the timing of the consultation and the communication methods used."

Medicare expansion of reimbursement for telemedicine also imposes limitations on the categories and qualifications for telehealth consultation to be covered, he notes. This can mean that investment in communication technologies in-house might not yield a return on investment. Providers have to make up the difference by charging already strapped healthcare consumers paying high premiums for insurance self-pay rates and by increasing their revenue generation efforts through third-party sponsorships and advertising, the latter of which is a risky proposition when dealing with personal healthcare matters, he says.

"To top it off, greater reliance on information systems creates what is perhaps the greatest exposure to consumers today: privacy and security. The risks include security breaches, identity theft, and consumer practices that sell information for marketing purposes without heed for privacy and dignity," Lebow says. "This requires coordination of legal oversight not only over electronic medical record systems but also for credit card processing, banking, and marketing communications. The disparate laws and regulatory oversight governing information practices across these industries neglect to understand that they are more linked than ever."

The growing use of telemedicine

also is raising more questions about the informed consent process, says **Jayme R. Matchinski**, JD, an attorney and officer with law firm Greensfelder, Hemker & Gale in Chicago. With several physicians and healthcare organizations potentially involved in a telemedicine arrangement, it is important to be clear about who is responsible for obtaining informed consent and when, she says.

"The question often comes to whose patient is it. Who is doing the informed consent and the billing?" Matchinski says. "Every state has its own telehealth laws, so if I have a physician with a patient in Georgia but the other provider is in another state, you have to figure out the scope of practice for that other professional. What is the scope of practice for that professional and are we compliant with the laws in both states?"

Another challenge involves prescription standards to address questions such as who will provide durable medical equipment and medications, she says. The parties involved in telemedicine should determine such answers before proceeding to avoid any reimbursement delays or conflicts with state laws, she says.

Matchinski also expects cybersecurity to be a growing challenge for healthcare risk managers.

"The government has been more aggressive in seeking out HIPAA breaches, not just electronically but in other ways also," she says. "States are taking a closer look at how you protect patient information, so I expect health information exchanges and how you protect that information to be a big issue this year."

States such as California and New York have passed consumer protection laws that may have major implications for healthcare organizations. The former's new consumer privacy laws are stricter than most, and the latter's new security requirements for financial institutions are the strictest in the country, Lebow says.

Also, Europe entered the fray by passing highly complex rules for those catering to overseas residents, he notes. Because companies operate nationally and sometimes internationally, stakeholders are advised to adhere to the strictest of standards even if the regulations within their own state differ, he says.

AN ONGOING CHALLENGE THAT ORGANIZATIONS WILL CONTINUE TO FACE THIS YEAR IS WHETHER AND HOW AVAILABLE DATA ARE USED TO MEASURE THE EFFECTIVENESS OF A COMPLIANCE PROGRAM.

Industry participants should of course look at the healthcare laws governing privacy and security. But they also need to ensure that they review consumer protection laws governing general privacy for consumers and the use of information for marketing purposes, he says.

"Further, healthcare providers should use online credit card processing companies that have their own direct relationships with the banking institution, so as to avoid going into the business of storing and managing credit card and financial data," Lebow says.

An ongoing challenge that organizations and compliance officials will continue to face this year is whether and how available data are used to measure the effectiveness of a compliance program and to proactively identify potential areas for change or improvement, says **Katie C. Pawlitz**, JD, partner at the law firm of Reed Smith in Washington, DC.

Organizations have access to more and more data related to their own operations and how they compare to their peers, Pawlitz notes. This could be internal data as well as external data, such as Medicare utilization and payment data or Program for Evaluating Payment Patterns Electronic Report data. This information can be very beneficial to organizations when analyzed appropriately, she says.

Such analysis can be used to fulfill an organization's obligation to engage in proactive compliance activities, like those outlined in the 60-day Overpayment Rule, Pawlitz says.

"At the same time, the availability of such data puts the onus on organizations to actually use it. Organizations that fail to engage in reasonable data analytics may do so at their own peril. This is because the government and qui tam relators also have access to data and are analyzing it themselves," Pawlitz says. "As such, compliance officials cannot simply focus on responding to issues as they arise, which is already a huge challenge. They must also be proactively monitoring data to identify if there are other issues that may be percolating."

The rapidly evolving privacy laws and regulations in the U.S. and abroad are presenting new challenges to healthcare organizations, says **Kimberly J. Gold**, JD, partner with the Reed Smith law firm in New York City.

Notably, she says, the California Consumer Privacy Act (CCPA), scheduled to go into effect on Jan. 1, 2020, provides for expansive individual rights and compliance obligations.

The CCPA contains several exemptions applicable to healthcare organizations, including for protected health information regulated by HIPAA, but the scope and applicability of these exemptions remain unclear, Gold says.

"We are still awaiting implementing regulations and further guidance from the California attorney general. Other states have proposed new privacy bills, and there remains uncertainty as to whether a privacy law will be adopted at the federal level that could pre-empt state privacy laws like the CCPA." ■

SOURCES

- Anjali N.C. Downs, JD, Epstein Becker Green, Washington, DC. Phone: (202) 861-1899. Email: adowns@ebglaw.com.
- Brad Fell, MD, Head of Compliance, Allied Physicians Group, Melville, NY. Phone: (866) 621-2769.
- Kimberly J. Gold, JD, Partner, Reed Smith, New York City. Phone: (212) 549.4650. Email: kim.gold@reedsmith.com.
- Michael B. Lampert, JD, Partner, Ropes & Gray, Boston. Phone: (617) 951-7095. Email: michael.lampert@ropesgray.com.
- Ron Lebow, JD, Senior Counsel, Health Law Group, Greenspoon Marder, New York City. Phone: (212) 524-5088. Email: ron.lebow@gmlaw.com.
- Jayme R. Matchinski, JD, Greensfelder, Hemker & Gale, Chicago. Phone: (312) 345-5014. Email: jmatchinski@greensfelder.com.
- Katie C. Pawlitz, JD, Partner, Reed Smith, Washington, DC. Phone: (202) 414-9233. Email: kpawlitz@reedsmith.com.

Tough Topics Addressed in Educational Rounds

A Massachusetts hospital has found that interprofessional educational rounds can be an effective way to discuss adverse events and other topics that might be difficult for some clinicians to address openly in the normal course of their work.

The rounds provide a structured, safe way for clinicians to address issues that can be emotional and stressful, says **Christine M. Rachwal**, MSN, RN, CCRN, clinical nurse specialist with Boston Children's Hospital. Those difficult issues are plentiful in a children's hospital, she notes.

The monthly, hour-long rounds are part of the Program to Enhance Relational and Communication Skills (PERCS), which also includes workshops. Participation is voluntary and offered to interprofessional clinicians from four critical care units, the cardiac catheterization unit, and intermediate care unit, Rachwal says. Topics are developed collaboratively.

"There were a lot of issues happening on the units that people wanted to talk about, and we wanted to make sure we allowed that opportunity in a guided, facilitated educational approach," Rachwal explains. "It's very different than a support group. This is much more of an educational format."

The rounds are effective because they are conducted in a learning format and with specific parameters, says **David M. Browning**, MSW, LICSW, co-founder of the hospital's Institute for Professionalism and Ethical Practice.

"The rules of engagement, in terms of how the time is protected and the safety provided for people to speak, is central to the success of the rounds because in a hierarchical healthcare environment people are not always open and honest in talking about topics they really care about," Browning says. "Creating an environment in which people can do that makes this special. It's learning in a different way than people are sometimes accustomed to."

The process starts at the beginning of each month with a planning meeting that involves facilitators, support staff, a registered nurse, and representatives from ethics, psychiatry, and other areas. There also are representatives from the hospital's parent advisory group.

Six units participate — four critical care, one acute care, and one intermediate care. The units rotate twice a year to bring their concerns to the table, highlighting what they would like to be addressed.

"We consider the suggestions and look for what people are going to get the most benefit from, produce an objective for the session later in the month, develop a title, and think about what experts from the institution we're going to invite to contribute to the discussion," Rachwal says. "One topic that had a

lot of interest was pediatric consent, with some parents not wanting their child to know what was happening. People were concerned about the legal aspects, so we invited legal to contribute."

A flyer is distributed to all the critical care units and then the rounds are held a few weeks later. Rachwal and Browning are usually the key facilitators, accompanied by the people asked to contribute to that month's topic. An administrative coordinator keeps the program on time, takes notes, and helps participants with continuing education credits.

Some sessions are conducted as group discussions, while others are organized with a whiteboard listing the key topics and staff concerns, along with potential solutions.

"People can see it in black and white and then discuss their own experiences. We always want them to leave feeling like they were presented with potential solutions and had their voice heard," Rachwal says. "The parents who participate are so important because we want to make sure we get all aspects and all viewpoints of a situation."

Participants are assured of confidentiality. The sessions last about an hour. At the end, the facilitators go around the room asking each participant to describe what they are going to take away from the meeting.

"We have found on some occasions that their answers to that question reveal we need to dive into this a little deeper with another round," Rachwal says.

The hospital originally held the rounds in a central conference space but found that attendance lagged because clinicians found it difficult to be away from their units. Now the rounds are held on the units, with as many as 30 participants.

Physician attendance also has been a challenge, Rachwal says. They are pulled in many directions, but attendance is improving with the use of "champion" physicians who believe in the idea and promote the program in the same way champion nurses promote it to their peers, she says.

The hospital described the program in a study available online at: https://bit.ly/2TEnifm. ■

SOURCES

- **David M. Browning**, MSW, LICSW, Institute for Professionalism and Ethical Practice. Boston Children's Hospital. Phone: (617) 355-5021.
- **Christine M. Rachwal**, MSN, RN, CCRN, Clinical Nurse Specialist, Boston Children's Hospital. Phone: (617) 355-6000.

Wrongful Delegation Can Happen Easily; Consequences Are Serious

Risk managers should educate nurses about the potential liability risks from wrongful delegation, which could threaten the nurse's career and expose the hospital.

Wrongful delegation occurs when a task is assigned to a worker who doesn't have the credentials to perform the task, says **Jennifer Flynn**, CPHRM, manager in the Healthcare Risk Management division of consulting firm Aon in Fort Washington, PA.

"Nurses are faced with this situation because of the push to cut costs and work with fewer people on staff, as well as the nursing shortage," Flynn says. "It becomes a liability issue for the nurse because even if he or she has been put in a situation in which they feel they have to delegate tasks to an unlicensed staff member to get the job done, ultimately they are responsible for what happens to that patient."

Effective delegation frees the nurse to focus on providing quality care to the patient rather than being bogged down with tasks that can be carried out safely by someone with less training, Flynn notes. Tasks that can be safely delegated are those that do not require nursing judgment, Flynn explains.

"Each patient is a case-by-case basis, and sometimes, it will be a moment-to-moment basis as to whether it is safe to delegate or not," Flynn says. "The nurse also has to consider the capabilities of the particular person that you are considering delegating this task to. Does that person have the competency to do what you're considering delegating?"

Communication is key to safe delegation, Flynn says. The nurse must not assume what the unlicensed staff member is capable of doing or has experience with, she says.

In most healthcare settings, the roles of staff members and associated tasks for those staff members are clearly defined by regulations (such as state nurse practice acts for registered and licensed nurses), organization policy, and job descriptions, notes **Bette McNee**, RN, NHA, clinical risk management consultant at insurance broker Graham Company in Philadelphia.

"Allowing care to be provided by an unlicensed worker who may not have the skills or experience with specific techniques is considered wrongful delegation and should be avoided at all costs," McNee says. "Nurses should get in the habit of asking themselves, 'Does this patient require special care that is beyond the typical or usual patient care?' If the answer is yes, the nurse must determine if the unlicensed worker or CNA [certified nursing assistant] is competent to provide the specialized care or task — as many would agree that a 'reasonably prudent nurse' would do so."

The nurse may always choose to perform the task him- or herself rather than determining competency, McNee notes.

"Typically it is not a true delegation issue like we see in the office setting where responsibilities are assigned as projects are planned. In healthcare, the roles and responsibilities are clearly defined: nurses take orders, administer medication and treatment, make observations or perform assessments, whereas unlicensed workers like CNAs or rehab aides feed, bathe, toilet, groom, and transfer patients," McNee says.

"The question of delegation — who is allowed to do what — seems to be a simple one, but that's not always the case."

The issue can arise when a task that is typically and appropriately completed by the lesser skilled or unlicensed worker is not appropriate in some circumstances. For instance, CNAs feed patients; it is a core responsibility of their position. However, if the CNA is assigned to feed a patient who had suffered a stroke, the patient must be fed in a particular way to prevent aspiration.

"If the nurse does not determine if the CNA is competent enough to feed this patient and the patient aspirates, the nurse's delegation of the task of feeding can come under fire," McNee says. "It actually isn't a delegation at all. If the nurse allows the CNA to feed the patient as he or she normally would — because it is their responsibility — without establishing the CNA's competency, the nurse is failing to undelegate the task."

Ambulation is also a core responsibility of CNAs, McNee notes. Issues can arise in a situation where a patient walks too quickly or has a tendency to lose balance. The nurse must determine whether the CNA has competency before allowing him or her to perform the task they were hired to do, she says. Failing to ensure competency before allowing the CNA to ambulate the patient is a liability risk for the organization as well as the nurse, she says.

Although CNAs are trained and assigned to feed, transfer, toilet, groom, and bathe, it is the nurse's responsibility to oversee the patient's care, and it is something that needs to be taken very seriously, McNee says.

A risk manager can help nurses avoid wrongful delegation by sharing this potential risk with all licensed staff, supervisors, managers, and department directors within the organization, McNee suggests.

"To be proactive, they can ensure that the organization measures the competency of CNAs or rehab aides to care for patients with various needs," McNee says. "It also makes sense to create a process so that CNAs or rehab aides are trained in the specific techniques required to care for each patient and are taught to request clarification of techniques before attempting to care for a patient who requires a specialized approach." ■

SOURCES

- **Jennifer Flynn**, CPHRM, Manager, Healthcare Risk Management, Aon, Fort Washington, PA. Email: jennifer.flynn@aon.com.
- **Bette McNee**, RN, NHA, Clinical Risk Management Consultant, Graham Company, Philadelphia. Email: bmcnee@grahamco.com.

DOJ Pursuing EHR Vendors for False Claims, Kickbacks

Electronic health record (EHR) company Greenway Health recently settled False Claims and Anti-Kickback charges with the U.S. Department of Justice (DOJ) for $57.25 million, less than a year after another vendor settled a False Claims case for $155 million. The cases should make risk managers more aware of the potential liability hospitals and health systems could face from using EHRs tied to fraud charges.

The DOJ could pursue criminal charges in the future, which could lead to hospitals being swept up in conspiracy allegations.

The DOJ alleged that Greenway caused its users to submit false claims to the government by misrepresenting the capabilities of an EHR product. Prosecutors also claimed that the company provided unlawful remuneration to users to induce them to recommend the product.

Assistant Attorney General **Jody Hunt**, JD, of the DOJ's Civil Division, explained in a public statement that the alleged fraud was related to provisions of the American Recovery and Reinvestment Act of 2009 that established the Medicare and Medicaid EHR Incentive Program to encourage "meaningful use" of EHR technology. Users could receive incentive payments if they adopted certified EHR technology and met certain requirements relating to its use.

The DOJ contends that Greenway falsely obtained 2014 Edition certification for its product when it concealed from its certifying entity that the product did not fully comply with the requirements for certification. Prosecutors cited several faults, including that Greenway's product did not incorporate the standardized clinical terminology necessary to ensure the reciprocal flow of information concerning patients and the accuracy of electronic prescriptions.

Greenway modified its test-run software to deceive the company hired to certify the program into believing that it could use the requisite clinical vocabulary, prosecutors alleged.

Government Claimed Kickbacks

The meaningful use incentive payments also required healthcare providers to provide patients with clinical summaries following office visits. The government alleged that Greenway was aware that an earlier version of the software, which was certified to 2011 Edition criteria, did not correctly calculate the percentage of office visits for which its users distributed clinical summaries and thereby caused certain users to falsely attest that they were eligible for EHR incentive payments.

"Greenway refrained from rectifying this error in order to ensure that its users would receive incentive payments," Hunt's statement explained. "As a result, numerous users of this earlier version of Prime Suite falsely attested that they were eligible for EHR incentive payments when, in fact, they had not met all necessary use requirements."

DOJ also accused Greenway of violating the Anti-Kickback Statute by paying money and incentives to its clients for recommending Prime Suite to new customers.

Greenway Health CEO Richard Atkin issued a statement noting that "The settlement is not an admission of wrongdoing by Greenway, and all our products remain [Office of National Coordinator for Health Information]-certified. This agreement allows us to focus on innovation while collaborating with our customers to improve the delivery of healthcare and the health of our communities."

DOJ Showing Aggressive Stance

Although the defendant in this case was a vendor, healthcare risk managers should take note of the DOJ's prosecution, says former assistant United States Attorney **Jason Mehta**, JD, now an attorney with the Bradley law firm in Tampa, FL.

"The Greenway Health settlement is reflective of the government's keen interest in focusing on compliance and accountability of healthcare companies of all stripes, be they clinics, hospitals, or even software developers," Mehta says. "From the same office that just months earlier announced another settlement with an electronic health record company, the U.S. Attorney's Office in Vermont is demonstrating a proficiency in software coding and meaningful use requirements."

For hospitals and health systems that rely on EHRs, the future is a bit uncertain, Mehta says.

"The government has not yet signaled an interest in pursuing customers who used faulty EHR systems," he says. "But given the government's aggressiveness to date, providers are not out of the woods yet."

A few lessons can be gleaned from this most recent settlement, Mehta says. First, most vendors like Greenway Health update their software with routine updates, many of which are focused on emerging compliance requirements. Therefore, customers of Greenway Health would be well-served by applying any software updates.

Second, companies focused on innovation would be wise to use this settlement as a warning and a reminder that all new innovative software, techniques, and procedures need to be fully vetted for compliance prior to deployment, Mehta says.

"Third, and finally, clinicians and hospitals alike would be wise to remember the old adage that an ounce of prevention is worth a pound of cure," he says. "Nowhere is that more true than in the world of modern regulated medicine."

Criminal Prosecution Possible

The Greenway Health settlement should worry hospital and health system risk managers, says **Sarah Hall**, JD, a former federal white-collar crime prosecutor and now senior counsel with the Thompson Hine law firm in Washington, DC.

"Hospitals and health systems that contract with EHR vendors and rely on their integrity should now be on notice that the biggest players in the healthcare fraud enforcement space — Main Justice, U.S. Attorneys' Offices, the FBI, and HHS-OIG — are looking closely at EHR companies," she says. "Although the Greenway case was resolved by the government civilly, these are the same enforcement agencies who can and do refer cases for criminal prosecution. DOJ is not mincing words. They are likely probing the EHR industry as a whole."

Healthcare organizations that contract with EHR vendors should pay attention to this settlement and use it as an opportunity to take a close look at their business arrangements with EHR vendors, Hall says.

"If the next EHR case goes criminal, the concept of conspiracy is a flexible one in the hands of a prosecutor," she says. "Healthcare organizations could be dragged into the criminal realm if they knew or participated in the use of noncompliant EHR products, had unusual business relationships with such vendors, or submitted false claims to Medicare, Medicaid, or other healthcare programs based on known faults with the EHR products."

Hospitals and health systems that contract with EHR vendors should audit their financial relationships with such vendors to ensure that there are no Anti-Kickback Statute issues at play, Hall says. Specifically, they should make sure neither they nor their subsidiaries are, or have, contracted with Greenway. Next, they should ensure that any EHR vendors they use are not providing them any money or incentives to recommend them to prospective new customers.

"In the Greenway case, these kickbacks were disguised as gifts, discounts, credits toward fees, and various Ambassador Programs and Reference Programs," Hall says. "Healthcare organizations need to drill down on the precise financial relationship that is actually happening on the ground and should consider using internal audit or compliance departments to do such investigation, or engage qualified outside counsel."

Don't Assume Vendor Compliance

Most healthcare organizations, including larger hospital systems that deal with large, established EHR vendors, assume that their vendors are fully compliant with the myriad healthcare regulations governing the industry, notes **Damaris Medina**, JD, an attorney with the Buchalter law firm in Los Angeles. The two EHR settlements show that is not always the case, she says.

"With this settlement, the government is sending a clear message that it has identified meaningful use and the use of EHR technology as an area of potential fraud, and it has committed resources to investigate and pursue EHR companies for improper conduct," Medina says. "Healthcare organizations have ultimate responsibility for their documentation and claims submission, their patients' health information, their relationships with vendors, and the representations they make to the government through the use of vendors' products."

While this settlement was directed at the EHR company itself, it is not difficult to envision a situation where an unwary healthcare organization contracts with a bad actor and is exposed to liability through its purported "knowledge" of the bad acts, Medina explains. The False Claims Act's definition of "knowledge" doesn't just include actual knowledge, she says. It also includes deliberate ignorance or reckless disregard of the truth or falsity of information. Intent is not necessary for False Claims liability, she notes.

"A healthcare organization's first line of defense is always to perform due diligence and run any contract and/or relationship it enters into through legal review and its compliance process. Even if providers were not aware of the alleged false certification issues, or the improper metrics formula allegedly used for incentive payments under the meaningful use program, a legal evaluation and compliance review by the provider prior to involvement in these 'Ambassador' and 'Reference' programs may have raised some important flags that would have caused the provider to ask more questions or otherwise reconsider doing business with the vendor," Medina says.

"Healthcare organizations, and especially hospital systems — which have substantial leverage with these companies — can also negotiate various safeguards into their EHR contracts, such as indemnity clauses, disclosures, and warrantees, and specific compliance clauses that can afford them some additional protection." ■

SOURCES

- Sarah Hall, JD, Thompson Hine, Washington, DC. Phone: (202) 263-4192. Email: sarah.hall@thompsonhine.com.
- Jason Mehta, JD, Bradley, Tampa, FL. Phone: (813) 559-5532. Email: jmehta@bradley.com.
- Damaris Medina, JD, Buchalter, Los Angeles. Phone: (213) 891-5224. Email: dmedina@buchalter.com.

HEALTHCARE RISK MANAGEMENT™

CME/CE INSTRUCTIONS

To earn credit for this activity, please follow these instructions:
1. Read and study the activity, using the provided references for further research.

2. Log on to ReliasMedia.com to take a post-test, then select "My Account" to view your available CE activities. First-time users will have to register on the site using the subscriber number printed on their mailing label, invoice, or renewal notice.

3. Pass the online tests with a score of 100%; you will be allowed to answer the questions as many times as needed.

4. After successfully completing the test, a credit letter will be emailed to you instantly.

5. After the test, your browser will be automatically directed to the activity evaluation form, which must be completed to receive your credit letter.

CME/CE QUESTIONS

1. **What does Anjali N.C. Downs, JD, an attorney with the Epstein Becker Green law firm in Washington, DC, say about the Eliminating Kickbacks in Recovery Act of 2018 (EKRA)?**

   a. It appears to have a broad reach, implicating all arrangements for laboratory services.
   b. It appears to be quite limited in scope and will not affect most organizations.
   c. It applies only to healthcare organizations based in California.
   d. It has been slated for repeal.

2. **Why does Michael B. Lampert, JD, partner with the Ropes & Gray law firm in Boston, say the move to value-based care is creating potential compliance problems?**

   a. Some laws meant to discourage fraud were created in fee-for-service healthcare.
   b. The additional recordkeeping requirements are burdensome.
   c. Fewer recordkeeping requirements leave less information to support claims.
   d. Insurers are more carefully scrutinizing claims.

3. **Who is ultimately responsible for the patient and can be held liable when a nurse delegates certain tasks to an unlicensed employee?**

   a. The unlicensed employee
   b. The nurse
   c. The director of nursing
   d. The employer

4. **What was one of the allegations from the Department of Justice against an electronic health record (EHR) provider?**

   a. It did not provide certification for its EHR product.
   b. It did not renew certification for its EHR product as required annually.
   c. It falsely obtained certification by concealing that the EHR product did not fully comply with the requirements.
   d. It falsely claimed that its certifying entity had certified the EHR product.

LEGAL REVIEW & COMMENTARY
EXPERT ANALYSIS OF RECENT LAWSUITS AND THEIR IMPACT ON HEALTHCARE RISK MANAGEMENT

$32.5 Million Award Affirmed for Patient Who Suffered Permanent Injuries During Childbirth

*By **Damian D. Capozzola**, Esq.*
The Law Offices of Damian D. Capozzola
Los Angeles

***Jamie Terrence**, RN*
President and Founder, Healthcare Risk Services
Former Director of Risk Management Services (2004-2013)
California Hospital Medical Center
Los Angeles

***Elena N. Sandell**, JD*
UCLA School of Law, 2018

News: A female patient suffered from a venous varix in her brain. The condition was determined non-life-threatening, but the patient's physician failed to note the condition on her list of current medical problems. When the patient became pregnant a few years later, the patient suffered immediate and serious complications after delivering her child, resulting in permanent injuries.

The patient's husband brought suit against the patient's primary care physician and his practice, alleging that the patient's primary care physician failed to note the condition and that this failure resulted in the patient's injuries. According to testimony, the injuries could have been avoided through a cesarean section delivery. A jury returned a verdict of $32.5 million, and the defendants appealed. The appellate court affirmed the results.

Background: The patient, a former teacher, exercise class instructor, and marathon runner, led an active lifestyle but began to suffer from persistent dizziness in 2004. When the patient sought medical treatment, an MRI revealed a venous varix in her brain. Although the venous varix was determined not to be the cause of her dizziness, the information was not noted on the patient's list of current medical conditions or problems by the patient's primary care physician despite the physician having received the report from the imaging center.

During the subsequent litigation, the plaintiff alleged that it should have been noted on the patient's "problem list" to alert her other treating physicians of potential complications that might arise. The patient was not informed that her condition could lead to complications during childbirth. Unaware of possible complications, the patient became pregnant in 2007 and gave birth to her daughter in 2008.

ACCORDING TO PHYSICIANS, THE PATIENT'S INJURIES ARE PERMANENT AND COULD HAVE EASILY BEEN AVOIDED THROUGH A CESAREAN SECTION DELIVERY RATHER THAN VAGINAL DELIVERY.

Approximately 12 hours after delivery, the patient experienced a sharp headache that indicated the rupture of her venous varix. The patient immediately underwent emergency surgery to remove part of her skull, but was insufficient to prevent injury. The patient fell into a month-long coma and, upon awakening, suffered significant and debilitating injuries: the patient's legs and left arm were paralyzed, her trunk muscles were severely impaired, and she experienced difficulty chewing, swallowing, and speaking. According to physicians, the patient's injuries are permanent and could have easily been avoided through a cesarean section delivery rather than vaginal delivery.

The patient's husband filed a lawsuit against the primary care physician and his medical practice, alleging that the physician's failure to document the results of the MRI and the venous varix condition constituted medical malpractice. The defendant physician and practice denied any liability and wrongdoing.

After a two-week trial, the jury found in favor of the plaintiff, awarding $32.5 million. The defendants appealed the decision and alleged that the damages should have been limited to the statutory limitation for certain charitable organizations pursuant to the applicable state's laws, that the plaintiff and his counsel misrepresented the amount of the patient's medical bills, that the plaintiff entered into an impermissible contingent fee agreement for consulting services, and that plaintiff's expert witness exceeded the bounds of the parties' pretrial memorandum. None of these attempts to undermine the liability and damages verdict were successful. The appellate court found against the defendants and held that the trial court had not abused its discretion in denying the defendants' post-trial motions, and that sufficient evidence had been presented to establish that the patient's future medical expenses would be at least $11 million.

What this means to you: In this case, the underlying medical malpractice stemmed from the failure of the primary care physician to note the cerebral venous anomaly (a cluster of veins that can rupture) on the records. This demonstrates the important need for accurate medical records, and that the failure to provide them can constitute action below the applicable standard of care. When a physician or care provider is informed of or discovers material relevant for inclusion within a patient's medical records, the provider should note it accordingly. The primary care physician here was copied on and thus informed about the venous varix but failed to document the condition.

Although such an anomaly is unusual to find in the brain and studies have shown that the risk of rupture may not decrease with cesarean section, the obstetrician needed that information to make changes in the obstetrical plans for this patient. Closer observation for changes in blood pressure, neurologic changes, complaints of headache, or nausea would have occurred evaluated based on the presence of the venous varix.

Consultation with neurologists and obstetricians familiar with this anomaly could have provided the patient's obstetrician the opportunity to evaluate the risks of a vaginal delivery. Now that electronic records are available for physicians across the continuum of care, these omissions are less frequent — but if they occur, such omissions are more likely to constitute malpractice.

One additional note for physicians and care providers is the shared responsibility that the physician has with the patient to make sure that the medical history is complete. A simple discussion between the patient and the obstetrician reviewing her medical history might have given the patient the opportunity to inform the obstetrician of the venous varix.

In addition to certain laws limiting the amount of damages recoverable by plaintiffs, there are other methods for physicians and care providers to reduce excessive, unfavorable verdicts. An award of damages must be supported by evidence, although the level of evidence required may vary and be subject to the discretion of the court or the jury. Here, the defendants disputed the amount of damages even after the trial court lowered the initial jury award. Referencing previous decisions, the court reiterated that damages are considered excessive when it may be assumed that the jury did not exercise sound discretion and was instead influenced by passion, partiality, or corruption.

The fairness issue arose after the jury returned with an interrogatory regarding the family's out-of-pocket medical expenses. Additionally, in his closing argument, the plaintiff's attorney misrepresented the amount of medical expenses the patient's family sustained. However, the defendants did not object to the statement when it was made and, furthermore, the judge instructed the jury that closing arguments were not to be regarded as evidence. Nevertheless, the jury returned an award that relied on the attorney's misrepresentation.

Thus, following the defendants' post-trial motion, the judge reduced the award to conform to the amount stated in the evidence presented during trial: approximately $3 million less than the amount incorrectly stated by the plaintiff's counsel during closing arguments. The defendants also unsuccessfully challenged the award as to the patient's future medical expenses, but the court found that there was sufficient evidence based upon the plaintiff's expert testimony and the patient's father's testimony.

To place this case in a more general context, physicians and care providers have a wide variety of defenses available in the event of a medical malpractice action. Some of those focus on the medical aspects of the case — such as challenging what exactly the applicable standard of care is — and others focus on legal requisites. In this case, the defendant physician and practice group attempted to minimize the damages award to a limit provided for certain charitable organizations, based on an applicable state law.

Unfortunately for the defendants, they encountered procedural errors that precluded this defense. The court noted that this limitation is an affirmative defense that must be pled and proved. However, the defendants failed to raise the limitation within the appropriate time, and the court therefore determined that the defendants waived the limitation. In fact,

the defendants sought to amend their answer to include this defense after more than four years from the beginning of litigation and two weeks after trial started. The defendants did not provide any explanation for the delay, and the court found that permitting the amendment would have resulted in prejudice to the plaintiff. The appellate court affirmed the decision and found that the defendants' errors resulted in the document not being actually offered into evidence during trial. While these procedural aspects are largely the responsibility of counsel, it is important for physicians and care providers to be aware of such possible defenses and the pitfalls of delaying or not raising them.

Finally, medical malpractice cases almost always require expert witness testimony. Given the nature of malpractice actions, it is common for each side to retain an expert physician to testify in support of its arguments. Issues about the scope of the expert's testimony can arise, and physicians and care providers may be successful in challenges limiting the scope of an opposing expert. In this case, the defendants unsuccessfully attempted such a challenge, claiming that the plaintiff's expert witness exceeded the scope of the subject matter boundaries established by the parties. However, the court found that the parties had anticipated that the expert witness would testify on multiple topics, including the changing nature of the size of a venous varix and that increased pressure caused by pregnancy substantially increases the chance of rupture. The expert witness also was intended to testify about causation: If a cesarean section would have been performed, the patient would not have sustained such injuries. The court found that defendants were properly notified of the subject of the expert's testimony and that no prejudice resulted from the testimony. Physicians and care providers should work closely with counsel from the outset of the case to evaluate not only their own expert witness's testimony but also to evaluate and seek to challenge or undermine an opposing party's expert witness. ■

REFERENCE

Decided on July 31, 2018, in the Appellate Court of the State of Massachusetts; Case Number 17-P-960.

Doctor Not Liable After Allegedly Concealing Outcome of Spinal Disc Surgery

News: A patient underwent spinal surgery but continued to suffer from pain in her mid-back. The patient subsequently sought treatment from a different physician and underwent a second surgery, which successfully eliminated her pain.

Following the second surgery, the patient brought a medical malpractice action against the first physician and alleged that the physician incorrectly performed the surgery and furthermore misrepresented the outcome of the surgery. The physician denied the allegations. A jury agreed with the defendant physician and found no liability.

Background: In 2009, a woman began experiencing back pain, originating in her mid-back and wrapping around her rib cage, extending upward to her sternum. After seeking treatment, a physician informed the patient that the CT angiogram and MRI showed a 4 mm disc protrusion at the T6-T7 level. The protrusion led to a compression in her spinal cord, causing the pain. The patient initially sought a more conservative treatment, but it did not alleviate the pain.

After the unsuccessful treatment, the patient scheduled a surgery with a physician to remove the protrusion that was causing the spinal compression. Following the surgery, the physician allegedly claimed the operation was successful and resolved the disc herniation. However, the patient continued to experience pain, and the physician ordered a new CT scan. According to the patient, the physician further asserted that everything had gone as planned and that the postoperative CT scan showed no compression in the patient's spine.

Despite the stated success of the surgery, the patient's pain persisted. The patient consulted another physician who, after analyzing the scans, identified a protrusion at the same level, which continued to cause spinal cord compression. The patient scheduled a second surgery on her spine, which was performed by the second physician approximately one year after her initial operation. The second surgery was a success and eliminated the patient's pain and discomfort.

The patient filed suit against the initial physician who performed the first spinal surgery, asserting four causes of action: professional negligence, intentional misrepresentation, concealment, and negligent misrepresentation. In her complaint, the patient stated that when she confronted the initial

physician about the continuing disc protrusion, he responded that he knew about it and had informed her. However, the patient disputed that she received such information and further alleged that her reliance on the initial physician's misrepresentation caused her to suffer months of ongoing and unnecessary pain, testing, and treatment. A jury disagreed that the initial physician's care fell below the applicable standard and found that the physician did not misrepresent or conceal information, thus absolving the initial physician of any liability. An appellate court affirmed the findings and conclusions.

What this means to you: Lessons from these events highlight the importance of corroboration, whether by a supporting colleague or staff, or by appropriate and thorough documentation. This case focused on the patient's allegation that the initial physician failed to inform her about the outcome of the surgery, in addition to the underlying claim that the surgery was unsuccessful. But the primary dispute was about communication, or lack thereof, and whether the physician concealed the results of medical scans to the patient.

While the patient claimed that the physician never informed her of the continuing protrusion, the physician and a colleague, who had also examined the patient during a follow-up visit and worked with the physician, corroborated that the postsurgical CT scans had been reviewed during the visit. Furthermore, the physician's colleague noted in the patient's record that the scan had been reviewed and that at the time it did not show any compression of the spinal cord. While the indentation at the T6-T7 level was not noted in the patient file, the physician's colleague admitted to seeing it and that in retrospect he should have included some annotation about it.

In this case, the defendant physician's ability to call his colleague who could testify to the fact that the patient was informed was critical to a successful defense. The further notation in the patient's record that the scan was reviewed undermined the patient's claim that she was never informed. Medical records serve a variety of functions, and while the primary function is to ensure that patients receive appropriate and necessary medical treatment, the records also serve as a useful tool in the event of medical malpractice litigation. It is far more difficult for physicians and care providers to assert that information was provided if there is a lack of contemporaneous documentation supporting those assertions.

The patient disputed the accounts of the defendant physician and the physician's colleague and instead claimed that neither physician informed her about the protrusion and that the initial physician had assured her that everything was fine. However, the patient did not produce any evidence of these events. The patient sought to introduce evidence of other litigation filed against the initial physician, which the plaintiff alleged were relevant for the purpose of proving the physician's intent and repetitive deceptive conduct because the allegations were similar in nature to the patient's allegations. The other litigation concerned separate incidents and other patients.

These events demonstrate one of the many important gatekeeping functions that judges and courts serve. While juries are ultimately charged with evaluating and weighing the evidence presented to them, judges determine whether the evidence reaches the jury. A physician's actions in a particular case are, of course, relevant for a jury to assess, but moving beyond that scope and to the physician's actions as related to other individuals may not be appropriate to present to the jury.

An additional consideration from the judge's and jury's perspective is the fact that unless an emergency exists, patients have the option to evaluate physicians and their practice well before seeking their care. Online data including physician grades, liability history, and patient satisfaction flood the internet. If the patient were aware of the multiple patient complaints and lawsuits filed against the surgeon, she may well have sought the assistance of a different physician. It is common for courts to disallow such evidence involving other patients and unrelated issues which have no bearing on the particular patient and issues present in the specific case at hand.

In this case, the defendant rightfully objected to — and sought to exclude — all such evidence from being presented to the jury on the basis that it would be more prejudicial than substantive. The court ruled in the physician's favor and excluded the inappropriate evidence. This presents an important lesson for physicians and care providers: A medical malpractice plaintiff may attempt to raise past litigation, including the mere fact that such allegations were raised, in an attempt to prove present liability. However, physicians and care providers should challenge the attempt to present such accusations, as those challenges often will be successful given the inherent unfairness and prejudicial effect. ■

REFERENCE

Appeal decided on Nov. 26, 2018, in the Court of Appeal of the State of California, Case Number B280399; trial decided on Dec. 21, 2016, in the Superior Court of the State of California, Case Number SC110925.

HIPAA REGULATORY ALERT

CUTTING-EDGE INFORMATION ON PRIVACY REGULATIONS

OCR May Alter HIPAA Rules to Ease Compliance, Care Coordination

The healthcare industry has complained about the difficulty of complying with HIPAA since the law was enacted. Now, the HHS Office for Civil Rights (OCR) is asking for suggestions on how to make HIPAA more manageable. What changes might actually happen remains uncertain.

OCR issued a Request for Information (RFI) seeking public input about how the HIPAA Privacy Rule could be changed to promote value-based and better coordinated care. *(Editor's Note: The RFI is available at: https://bit.ly/2iVERG4.)* OCR's effort to resolve frustrations with HIPAA is long overdue, says **Joseph A. Dickinson**, JD, partner with Smith Anderson in Raleigh, NC.

"HIPAA, as it has evolved, has gone too far. It is inhibiting the sharing of information for purposes of healthcare treatment," he argues. "We see it every day with doctors including fears of HIPAA liability in their healthcare process, sometimes not fully sharing information with other healthcare professionals that might actually be pertinent and needed to provide the best care."

Meanwhile, there is a serious problem in the industry with data breaches and healthcare organizations not taking their obligations seriously, Dickinson says. OCR's challenge will be to change the law in ways that ease the unreasonable burden without letting organizations off the hook if they do not make reasonable efforts to comply.

"I think OCR is going to cut back on the fundamental obligations to protect patient privacy up front, but making some changes on the other end so that once they have that protected data they can share it with other providers to get the best care for the patient," Dickinson says.

The OCR's RFI focuses on how HIPAA rules can be revised to facilitate coordination of patient care among and between providers, explains **Eric D. Fader**, JD, an attorney with the Rivkin Radler in New York. Although HIPAA became law in 1996, Fader says not everyone understands certain aspects of the rules. Thus, some healthcare providers, particularly their clerical employees, sometimes find it easier not to cooperate promptly with a patient's or another care provider's request for records while using HIPAA as an excuse.

The Treatment, Payment, and Healthcare Operations (TPO) exception to the Privacy Rule continues to be difficult to grasp for some, Fader says. The TPO exception permits (but does not require) the sharing of patients' protected health information (PHI) for purposes of care coordination. Fader says requests for PHI from one unrelated provider to another often are not handled with the same degree of urgency.

"The OCR has surely heard anecdotally of many instances where requests for information for treatment purposes were either not complied with at all, whether through a misunderstanding of what HIPAA allows or for workload reasons, or due to an unwillingness to cooperate with the requesting party," Fader says. "It appears that the OCR is considering how to make sharing PHI for purposes of treatment ... more mandatory than permissive, a goal with which I agree."

The other sections of the RFI are mostly variations on the same theme, Fader says. They include consideration of shifting some provisions of HIPAA from "disclosure of PHI is permissible if ..." to "disclosure is required under these circumstances."

Fader predicts care coordination, case management, quality assurance, and other activities will be easier if healthcare providers understand that they do not need to be concerned about disclosing PHI to another party that is subject to HIPAA already while also recognizing the need to handle requests promptly.

"Just as the OCR continues its enforcement activities when healthcare providers inexplicably still fail to comply with HIPAA after all these years, and just as they continue to put out press releases regarding settlements that are clearly intended to be educational for the provider community, the OCR has clearly recognized that more education is necessary to improve

sharing of patient information so that the system will work better overall," Fader says. "[OCR] seems to be prepared to make this a priority in 2019."

HHS started an initiative to enhance care coordination, but HIPAA has proven to be an obstacle, says **Richard Trembowicz**, JD, associate principal with ECG Management Consultants in Boston. Healthcare providers are hindered by cumbersome documentation of authorization to share and fear of extensive liability if information is inappropriately shared with third parties, he says.

"Simply put, the cost of documentation of authorization of access and delivery of PHI and risk of error in information management both increase if more individuals are authorized to have access to PHI, especially if the rules have lots of exceptions or nonstandard processes," Trembowicz explains. "CMS is also concerned that the time period within which a provider must respond to an individual's request for the sharing of PHI is too long, making the information value stale by the time it is shared."

HHS has posed 54 subjects for public comment to obtain insight on how changes to the rule could affect all involved in the care delivery process. Trembowicz notes that several questions seek feedback on the additional provider burden should HHS require providers to respond to individual requests for PHI faster than current law and regulations require. This will necessitate providers to devote additional resources to searching for, copying, and delivering the requested information to the individual, he says.

"It also begs the question of whether format of delivery, such as electronic, will be required, and whether the provider has a responsibility to deliver the information to other third parties as directed or requested by the individual," Trembowicz says. "All of this will cost money, and HHS provides no guidance on whether it will compensate providers for the additional costs." In addition, HHS is seeking feedback on the authorization process to release information, various exceptions, and effects on business associates with which the provider conducts business, including the security practices and documentation of authorizations to release information.

"The greatest concern of providers is that HHS will issue new unfunded mandates that increase the cost of medical care without compensation," Trembowicz says.

Several proposals for which OCR seeks feedback deserve special mention, according to **Kristen Rosati**, JD, an attorney with the law firm of Coppersmith Brockelman in Phoenix. First, she says the focus on including nontraditional providers and social service agencies in data sharing is important to managing care. There is an increasing recognition that the social determinants of health, such as the availability of food, counseling, and secure housing, significantly influence an individual's ability to manage a chronic condition or to improve after an acute health episode.

"Second, the industry should support OCR's focus on sharing information with family members and caregivers to address the opioid crisis and serious mental health issues," Rosati offers. "Family members and caregivers play an essential role in getting people with additional problems to treatment and in helping them manage their care. They often are as important to the treatment team as the physicians and nurses."

However, Rosati notes that OCR also solicits feedback on a proposal that would increase obstacles to data sharing. OCR has asked for comment on requiring HIPAA-covered entities to include information in an "accounting" about disclosures from electronic health records that are made for treatment, payment, and operations purposes. An accounting is a list that covered entities must provide to an individual on request, which includes information about disclosures of that individual's health information for purposes other than treatment, payment, and operations, Rosati explains.

"It's incredibly burdensome even under the current scope of the rule. Adding to that requirement creates more burden without much benefit. It also is not technically feasible to do automatically, as electronic health record systems do not capture the information that would be required in an accounting," she says. "We hope the industry pushes back on this proposal."

It is always difficult to predict how HIPAA regulations might change, says **Roy Wyman**, JD, partner with Nelson Mullins in Nashville, TN. Agencies like HHS generally avoid making changes to regulations, as such edits require lengthy administrative and public review and can end up causing as much damage as good, Wyman says.

However, the Trump administration emphasizes reducing the burdens of regulations. For example, the 21st Century Cures Act requires HHS to develop a plan to reduce regulatory and administrative burdens on the use of health IT and electronic health records. The Cures Act mostly targeted areas outside HIPAA, but the draft strategy for the Cures Act includes criteria that also could be used in any HIPAA simplification, Wyman explains.

The draft strategy says changes should be achievable within the near-to-medium term (a roughly three- to five-year window). It also says HHS should be able to either implement these strategies through existing or easily expanded authority or should have significant ability to influence the implementation of these strategies.

HHS may be reticent to take any actions perceived as watering down privacy protections, but some provisions may be ripe for change because they are not related to individuals' rights, Wyman explains.

"For example, the rules for when a hospital or provider can disclose information are complex and often require professional judgment," Wyman says. "More common sense and bright-line rules would simplify the process for sharing information with relatives and friends of patients and understanding when another individual or estate can act on behalf of the individual."

Other areas are largely invisible to individuals and privacy advocates but are complex. Such areas can cause unintentional violations. Some examples include sharing health information for "healthcare operations," public health, and research purposes.

"The ability to disclose information for these purposes is more complex and limited than sharing information for treatment or payment purposes," Wyman explains. "A simple guideline allowing entities to share information for operations of the sender or the receiver or for public health and research purposes, subject to the other rules of HIPAA, is a relatively simple fix that might receive relatively narrow complaints from privacy advocates. Such simplification also might promote the quality and efficiency of patient care."

Similarly, Wyman notes that the rules and definitions for Affiliated Covered Entities, Organized Health Care Arrangements, and hybrid entities create a legal tangle. These rules permit various types of arrangements and entities to comply with HIPAA, yet they can create administrative and training burdens. "Simplifying these rules could largely eliminate these definitions while permitting covered entities and business associates to be joined and divided in ways that seem most appropriate to the entity so long as those receiving health information comply with HIPAA and maintain the security of the information," he says.

Wyman believes the Security Rules also need a significant overhaul. "Many of the requirements overlap, contain confusing terms, and are mostly useful to assure consultants remain in business. The regulations could use a good review to reduce and consolidate many of the requirements, make sure that the requirements are understandable to the technologically naïve, and are more user-friendly," Wyman offers. "For example, the Security Rules include three different sections that address access control. Some sections of the regulations are deemed 'required,' and others are 'addressable,' yet all of them must be considered. A clearer description of what is required would eliminate a huge amount of confusion."

While technically outside of HIPAA, Wyman says rules about the protection of information held by mental health and substance abuse providers have created enormous burdens. The "Part 2" rules (42 C.F.R. Part 2) originally predated HIPAA as well as the internet. Although these rules were updated recently, they remain burdensome, according to Wyman.

"Unfortunately, the increased burden on these providers has made it very difficult for them to share information with other providers, participate in health information exchanges, or generally function in a data-intensive world," he laments. "A wholesale annexation of Part 2 into HIPAA seems unlikely, but the two sets of regulations could be better harmonized. For example, Part 2 could create an exemption that would allow sharing of data with a covered entity or business associate of a covered entity under HIPAA based either on a written agreement or particular requirements on the receiving entity written into the regulations. The requirements on the receiving entity might be similar to how covered entities treat psychotherapy notes under HIPAA."

OCR is asking the public for ways to modify the HIPAA regulations specifically to drive cost savings and value, which are most commonly expected to come from the development of coordinated care platforms, says **Jeff Drummond**, JD, an attorney with Jackson Walker in Dallas. HIPAA is naturally obstructive to care coordination. Any efforts at care coordination naturally assume ready exchange of patient information among providers, payers, and others involved in the care of the patient (or the patient population). Meanwhile, HIPAA's focus on privacy and security generally limits information sharing, according to Drummond. HIPAA allows for such sharing of patient medical records, but Drummond believes too many people in the healthcare industry do not understand HIPAA and are afraid of it. Thus, they refuse to share information even though HIPAA would allow it.

"Another major problem is that given the combination of the Facebook and other social media platform privacy issues all over the news, as well as the daily reports of major breaches of personal and medical information, many people are too afraid that their medical record privacy will be abused," he explains. "People fear for their privacy, so they don't want their information released, even though releasing the information in an appropriate manner would actually improve their healthcare and the overall cost of healthcare."

Drummond says these problems cannot be fixed by changing HIPAA because as currently structured, HIPAA would work to allow appropriate information exchange for care coordination and value-based healthcare. "Thus, I do not see any major changes being made to HIPAA," Drummond says. "However, given the push for regulatory change, and the need to be seen as doing something, I would expect some tinkering around the edges." Here is how Drummond expects to see OCR change HIPAA:

• Minor tweaks to the definition of "healthcare operations" to clarify and

possibly expand the ability to share PHI for population health, emergencies, and value-based care initiatives;

• Minor clarifications regarding "personal representatives" and when parents are (or are not) treated as such;

• Specific language (more likely guidance than changes to the actual text of the regulations) addressing uses and disclosures in the mental health and substance abuse arena;

• Revisions to the "accounting of disclosures" requirements to streamline the process by eliminating much of the requirement;

• Finalization of the rule allowing individuals to share in the fines levied by OCR for a HIPAA breach;

• Specific language addressing when a ransomware attack (or similar technology-driven incident) is a reportable breach.

Drummond says some commentators will ask for removal of the requirement that directs patients sign an acknowledgement receipt regarding the Notice of Privacy Practices when they first go to their doctor. However, he does not think that will occur. "It would definitely remove a noticeable burden on both providers who have to print out notices, ask for signatures, and keep track of them. Ultimately, that's a small burden to make sure that providers actually provide the notice," he says. Patients have an opportunity to think about how their information is going to be used and disclosed. Ultimately, I think [OCR will] leave it in place as is." The biggest effect from any changes may involve the increasing use of technology in the transmission of patient data from one healthcare provider to another, says **Patrick Pilch**, managing director and national leader for BDO Healthcare Advisory's Center for Healthcare Excellence & Innovation. "We're seeing more care being directed over smartphones, for example, so OCR may change the requirements for providers who have not been connected electronically in the past," he offers.

"That could have a big impact and would change HIPAA in a way that acknowledges how healthcare delivery has changed in the past 20 years. It's that kind of thing that frustrates people who are trying to comply with HIPAA but the law doesn't seem to fit with how things are done in the real world." ■

HIPAA Requires Security for Printers, Just Like Other Servers and Endpoints

HIPAA security requires protection for servers and various endpoint devices. However, many healthcare organizations do not realize printers need the same attention.

Most covered entities and business associates do not appreciate how printers have evolved from "dummy copiers" to today's complex business machines that include multiple servers built directly into them, explains **Jim LaRoe**, CEO of Symphion, a software and services company in Dallas. The competition among printer manufacturers has driven the inclusion of web servers, file transfer protocol servers, fax servers, huge hard drives, and many other advanced capabilities, he notes. Yet, printers, unlike standalone servers, are maintained outside of data centers without the physical and technical safeguards that are common to data centers.

"They are also managed by nonsecurity, non-IT professionals, not the heavily credentialed system administrators like in data centers, and are not included in IT policies and procedures," LaRoe adds. "Moreover, printers, like laptops, are mobile throughout the enterprise. They are often on wheels."

HIPAA's general mandates require covered entities to ensure the confidentiality, integrity, and availability of PHI the business creates, receives, maintains, or transmits. HIPAA also requires covered entities to protect against any reasonably anticipated threats or hazards to the security or integrity of information. "Printers in hospitals clearly 'create, receive, maintain, and/or transmit' electronic PHI," LaRoe notes. "Moreover, even the most cursory examination of reasonably anticipated threats and hazards to the security and integrity of that ePHI trigger the HIPAA mandates to protect printers."

Specifically, HIPAA requires covered entities and business associates to assess current security and risks for ePHI in the entire enterprise. That includes the risks presented by the printers and implementation of a security plan, policies and procedures, and controls that address vulnerabilities and risks. The entity must monitor, record, and evaluate implemented security settings to ensure the security plan and controls are maintained vigilantly, according to LaRoe.

"Neither hospitals nor enterprises are dealing with network printers correctly. That makes them one of the biggest security threats for 2019, especially considering that breaches are getting more costly," LaRoe warns. "Since every printer on a print fleet can provide hundreds of vulnerabilities, and many hospitals can have thousands of printers, the message is clear. Even though printers have been here for years, they ... must be protected like the servers that they are, with automated IT asset life cycle management and continuous cyber hardening." ■