HEALTHCARE RISK MANAGEMENT™

ReliasMedia.com

THE TRUSTED SOURCE FOR LEGAL AND PATIENT SAFETY ADVICE SINCE 1979

Relias Media

APRIL 2024 Vol. 46, No. 4; p. 37-48

Patient and Family Complaints Require Careful Response

Complaints from patients or family members are commonplace in healthcare, but knowing how to respond is not always clear. Some complaints will be trivial or unfounded, while others may indicate a serious patient safety issue or an incident that could lead to litigation and liability.

Risk managers can help channel those complaints in the right direction by helping frontline staff know how to respond, as well as when and when not to escalate the complaint.

There is no magic answer to what to say in response to a complaint, says **Paul D. Werner**, JD, an attorney with Buttaci Leardi & Werner in Tarrytown, NY. It is impossible to predict how the complainant will react to anything because the situation often is quite charged and dynamic.

"While it can be frustrating to not have a script when addressing complaints, the lack of a specific methodology also gives those responding to the complaint the ability to adapt to the specific circumstances," Werner says. "Anyone who may potentially be responding to a complaint in the healthcare context should be trained on the basic do's and don'ts, but also trained on substantive matters that will afford them the ability to review and react to the situation."

Werner advises clients to avoid making concessions or direct apologies for actions or behaviors and instead focus on understanding and empathizing with the complainant's situation. For example, rather than directly conceding that an error was made when talking with a complainant, Werner often advises clients to apologize for the inconvenience the complainant perceives or the problem the complainant is mentioning.

"By way of a specific example, I advise clients to say, 'I'm sorry to hear that you're experiencing discomfort,' or 'I'm sorry you're surprised by the fact that you were billed for that

EXECUTIVE SUMMARY

Healthcare organizations should have processes for responding to complaints from patients and families. The nature and seriousness of the complaint will dictate how much of a response is required.

- Clinicians and other staff should be trained in the proper response to complaints.
- Always be courteous and nonconfrontational when responding.
- Some complaints should be escalated to risk management for further investigation.

service,' as opposed to 'I'm sorry that happened to you,' or 'I'm sorry for that error.'" Werner explains.

Documentation Is Key

Any complaint should be fully documented in the patient's chart. To the extent a complaint is received in writing, that writing should be preserved in the file as well. Any audio or video recordings of the complaint, if they exist, also should be preserved.

In addition to documenting the complaint, any actions taken in response to the complaint should be documented, Werner says. If an internal investigation is conducted, that should be done with the assistance of counsel to ensure completeness and to protect privilege.

Lend a Sympathetic Ear

There should not be much difference in how clinicians and administrators respond, Werner says. Because clinicians are much more likely to receive complaints in person with the complainant face-to-face, clinicians need to maintain composure and provide thoughtful, calculated responses.

When hearing a complaint in person, it is recommended that the clinician simply listen to the complaint, acknowledge that it has been made, and assure the complainant that they will investigate and respond, Werner advises. Off-the-cuff responses, especially when there is the potential that professional judgment or skill is being questioned, often escalate things unnecessarily.

"The best tool in the toolbox for de-escalating a situation is being sure to listen to complaints, not simply hear them. Listening to and understanding the complaint allows you to provide a more thoughtful and complete response," Werner says. "In my experience, when the first response to the complaint is insufficient or perceived as a 'blow-off,' complainants are much more likely to press on."

Healthcare professionals should be receptive, empathetic, and sympathetic to anyone who is complaining, says **Eric S. Strober**, JD, partner with Rivkin Radler in New York City. It is normal for patients and families to want everything to go perfectly right every single time, and healthcare workers know that is not reality, he notes. That may lead to frustration with a complaint that seems unrealistic, but healthcare staff should nonetheless respond in an understanding way.

"If you address it and sympathize with the complainer's point of view and try to make sure that there's no harm done, then that's the best you can do under those circumstances. I don't think being defensive and knee-jerk reactions are the best way to go," Strober says. "You're not going to calm anybody down or assuage any kind of concerns by getting immediately defensive. In fact, you could just inflame matters that way."

Not every complaint needs to be escalated to risk management or nursing administration, but some do, Strober notes. A complaint about the response time for calling in a prescription or how long a patient had to sit in a room is just a garden-variety dissatisfaction with the realities of medical care in America in 2024.

"Those don't need to be reported to risk management. If there's no adverse event and no injury or no harm that has come to a patient, then it doesn't seem like there's a need to report anything," Strober says. "But if somebody was inadvertently stuck with a needle while someone was trying to draw blood — sure, report that."

Streamline the Response Process

Providers should have a streamlined process for responding to patient complaints, says **Aubrey B. Gulledge**, JD, an attorney with Baker Donelson in Memphis, TN. All complaints that rise to a level of severity to pose a threat of litigation or a threat to safety should be directed to risk management as soon as possible. The complaint should be acknowledged in a timely and conciliatory fashion, and the response should reflect that the provider takes the complaint seriously and is investigating.

Clinicians and administrators should consider that written communications with patients and their families are discoverable in litigation, Gulledge notes. Any complaint response should not include overreaching promises of remedial action, legalese, or medical jargon.

"Providers should be cognizant of privacy and confidentiality concerns when responding to complaints, and responses should not reference specific individuals," she says. "Providers should never comment regarding whether there was any lack of compliance with the standard of care applicable to the provider, or whether there was a perceived lack of compliance with policy or regulations. The responses should avoid commentary that could expand the facts involved in the complaint."

Risk management should have a process for documenting patient

complaints that includes the date of the complaint, the name of the person complaining and/or patient name, indication of who received the complaint, the content of the complaint, an indication of whether the complaint was written or verbal, and recommended follow-up, Gulledge says.

Gulledge notes that the necessary action depends on the nature of the complaint and the potential effect on the patient, other patients, and the public. When patient safety is at issue, engaging all stakeholders to take appropriate immediate action is imperative.

Follow-up communication with the patient and/or family should always happen, and in severe instances, risk management should be aware of potential third-party investigation, she says. The follow-up should acknowledge receipt of the complaint, and should occur upon completion of the investigation.

Both clinicians and administrators should engage their legal representatives and risk management professionals when they become aware of a patient complaint that involves patient safety issues and/or could turn into litigation, Gulledge advises. Clinicians should indicate that they have forwarded the complaint to management. Clinicians who are not in management positions should proceed with the direction of management and/or legal according to the department's policies and procedures. They should document in the medical record if they have personally received a complaint but should not document any communications with risk management or discussions regarding remedial action.

"We often find that the reason for litigation is the lack of understanding of what happened to the patient. Clinicians who take the time to explain disease processes and answer questions when there is an unexpected outcome are less likely to be sued," Gulledge says. "Taking time with patients and family members and not appearing to be in a hurry or cut them off when they ask questions will help avoid litigation."

Prompt and frequent communication with the patient or family is the most critical component of attempting de-escalation, Gulledge notes. A written record of acknowledgment, investigation, response, and follow-up is a powerful tool in ensuring a comprehensive response to complaints and best efforts to avoid future litigation. "This communication is the best way to promote patient satisfaction and gain, maintain, or regain patient and family trust," she says.

Do Not Admit Wrongdoing

From the perspective of litigation and complaints of medical incidents that have resulted in harm, the first step in responding to a complaint is to take it seriously and to show appropriate empathy without admitting to any wrongdoing, says **Bill Bower**, senior vice president with Gallagher Bassett in Rolling Meadows, IL, which provides healthcare professional liability claims and risk management consulting. Previously, Bower was chief risk officer at a major health system. Patients and family members should be advised that their complaint will be investigated, and that the institution will get back to them.

Many organizations have a disclosure policy or protocol that dictates the methods by which the institution will respond, Bower notes. Internally, complaints should be directed to the risk management department or to the particular body within the organization that is charged with clinical investigations of incidents. Often, this will allow for a determination of whether the complaint arises from an incident that might provide an opportunity for process improvement. This will lead to routing to the appropriate team — perhaps risk, patient safety, or process improvement. In addition, a complaint should be directed to those within the organization who are charged with notifying insurers of events that could result in a claim.

"If there are artifacts or evidence involved in the event — video coverage, retained foreign bodies, pathology, etc. — it is essential that such evidence be preserved. If an investigation reveals further evidence, such as text messages, these must also be preserved," Bower says. "Oftentimes, if the event is of a certain magnitude or litigation seems likely from the start, retention of counsel can be employed to begin an analysis from that perspective and to gain attorney-client privilege where feasible. Privilege may also be afforded under the Patient Safety Act as patient safety work product, if applicable." ■

SOURCES

- **Bill Bower**, Senior Vice President, Gallagher Bassett, Rolling Meadows, IL. Phone: (630) 773-3800.
- **Aubrey B. Gulledge**, JD, Baker Donelson. Memphis, TN. Phone: (901) 577-2218. Email: agulledge@bakerdonelson.com.
- **Eric S. Strober**, JD, Partner, Rivkin Radler, New York City. Phone: (212) 455-9560. Email: eric.strober@rivkin.com.
- **Paul D. Werner**, JD, Buttaci Leardi & Werner, Tarrytown, NY. Phone: (609)799-5150. Email: pdwerner@buttacilaw.com.

HHS Proposes Cybersecurity Requirements for Hospitals

The Department of Health and Human Services (HHS) recently released a concept paper outlining its cybersecurity strategy for the healthcare sector, focusing specifically on strengthening resilience for hospitals threatened by cyberattacks. HHS outlined four pillars for action, including new voluntary healthcare-specific cybersecurity performance goals.[1]

Cyber incidents in healthcare are increasing. HHS reported a 93% increase in large breaches reported to the Office for Civil Rights (OCR) from 2018 to 2022 — from 369 incidents to 712. There was a 278% increase in large breaches involving ransomware.[2]

"The healthcare sector is experiencing a significant rise in cyberattacks, putting patient safety at risk. These attacks expose vulnerabilities in our healthcare system, degrade patient trust, and ultimately endanger patient safety," said HHS Deputy Secretary **Andrea Palm**. "HHS takes these threats very seriously, and we are taking steps that will ensure our hospitals, patients, and communities impacted by cyberattacks are better prepared and more secure."[2]

The HHS concept paper outlines these initiatives:

- **"Publish voluntary Healthcare and Public Health sector Cybersecurity Performance Goals (HPH CPGs).** HHS will release HPH CPGs to help healthcare institutions plan and prioritize implementation of high-impact cybersecurity practices."
- **"Provide resources to incentivize and implement cybersecurity practices.** HHS will work with Congress to obtain new authority and funding to administer financial support and incentives for domestic hospitals to implement high-impact cybersecurity practices."
- **"Implement an HHS-wide strategy to support greater enforcement and accountability.** HHS will propose new enforceable cybersecurity standards, informed by the HPH CPGs, that would be incorporated into existing programs, including Medicare and Medicaid and the HIPAA Security Rule."
- **"Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity.** HHS will mature the Administration for Strategic Preparedness and Response's coordination role as a 'one-stop shop' for healthcare cybersecurity which will improve coordination within HHS and the federal government, deepen HHS and the federal government's partnership with industry, improve access and uptake of government support and services, and increase HHS's incident response capabilities."

More Regulatory Issues Could Emerge

Hospitals are grappling with unprecedented levels of cybersecurity issues and might welcome a higher level of regulation, says **Jolie Apicella**, JD, partner with Wiggin and Dana in New York City. However, that could come with new, emerging legal and regulatory issues on top of the regulations that they already face.

"HHS's mission here is to improve overall cybersecurity practices and build up the resiliency of the programs. These cybersecurity threats are really criminal operations, so hospitals have to now implement the absolute best cybersecurity practices. Not only that, but they have to live up to them, which is a very difficult thing to do," Apicella explains. "There could just be a slip-up, there might not even be any exposure or any sort of leaks that come from that, but they can then be on the hook."

The concept paper tells healthcare organizations where HHS is setting its priorities. "They're definitely working as hard as they can to improve the overall cybersecurity practices of hospitals because they are some of the most vulnerable targets," Apicella says. "They want to publicize any vulnerability that the hospitals may have as a way for the public to feel comfort that the hospital would be held accountable."

The concept paper draws attention to OCR's recently updated telehealth

EXECUTIVE SUMMARY

A concept paper from the Department of Health and Human Services (HHS) provides a cybersecurity strategy for healthcare organizations. The voluntary goals could become requirements soon.

- Cybersecurity incidents continue to increase every year.
- HHS will establish voluntary cybersecurity performance goals.
- Telehealth disclosure is noted in the paper as a particular concern.

guidance, notes **Jason Johnson**, JD, partner with Crowell & Moring in New York City. Along with guidance from the Federal Trade Commission, the HHS concept paper signals a joint collaborative effort that health organizations should heed.

"For telehealth, this is really the first significant paper that's put together a bunch of items on the telehealth side to provide some concrete information as to the use and access of telehealth," Johnson says. "During COVID, there was discretion from OCR around enforcement, and now we've kind of moved into the next phase where entities need to pay attention to what OCR is saying about this."

A key concern should be ensuring that the organization provides full disclosure to individuals, Johnson says. "It's important that your patients understand the privacy and security protections in place, and the risks that go along with that. I think that's a little bit of a significant deviation from what we've seen in the past," he notes. "This puts the burden on these entities to provide additional information and disclosure to those individuals that is in line with what you see outside of healthcare. I don't think a lot of healthcare entities probably are very well versed on that."

Voluntary Could Become Mandatory

The cyber performance goals to be developed by HHS would be voluntary at first but may become requirements soon, says **Kirsten Mickelson**, cyber practice group leader with Gallagher Bassett in Rolling Meadows, IL, which provides healthcare professional liability claims and risk management consulting.

"There are references in the proposal which are signaling that they will become requirements as early as this year. It builds on the Biden administration's national security strategy and serves as an introduction to HHS's own cybersecurity strategy," Mickelson explains. "I think it's significant because it offers insight to the healthcare sector into the more active role HHS will probably play in the cybersecurity space."

Through Sector Risk Management Agencies, HHS would be responsible for sharing cyber threat information and intelligence with the healthcare sector, but then also provide technical assistance, guidance, and resources to comply with the data security and privacy laws.

"This is coming from the highest level," Mickelson says. "It is significant in that sense because it demonstrates the level of involvement HHS will have with the government and the current administration in terms of sharing the threat intelligence. It shows that the overall goal is driving enhancements to critical infrastructure security."

HHS is signaling that they are holding healthcare organizations responsible for breaches, says **William P. Dillon**, JD, shareholder with Gunster law firm in Tallahassee, FL. Regulators may have had more sympathy in the past because organizations were up against sophisticated hackers with quickly emerging technology, he says.

"Then, they looked and said they failed to conduct a risk analysis, they didn't have policies or procedures in place to regularly review information system activity. They're pushing the same thing that they've been saying for years, and if people aren't adhering to that, I think OCR is taking the position of saying, 'We're going to have to do a two-pronged approach,'" Dillon says. "They're continuing to do education, but now they're holding some people's feet to the fire."

The cybersecurity plan does not seem to address one key failing in the government's enforcement of existing requirements, says **Iliana L. Peters**, JD, shareholder with Polsinelli in Washington, DC. Previously, Peters was acting deputy director for HHS and enforced HIPAA regulations. HHS responds vigorously to self-reported cyber breaches but does little to audit compliance and find unreported incidents, she says.

"All I see — at least for now, and I'm hoping that that will change — is increased enforcement against those entities who are doing something right. They're not doing everything right, but they have compliance programs and they're reporting breaches," Peters says. "Some of the enhanced goals are already required by law, so I'm a little confused about how that is an enhanced goal when it is something that arguably they should already be doing."

With the increased risk of cyber threats, cyber insurance is much harder to get now, and the insurers want to see more proof that the organization is taking adequate steps to protect against attacks, Peters says.

"You have to be investing money into understanding what your risk landscape looks like. That is risk analysis, risk management, implementation of really good controls, technical controls, data loss prevention, multifactor authentication — all of those things," she says. "You're never done with cybersecurity preparedness because the threats are constantly changing." ■

REFERENCES

1. U.S. Department of Health and Human Services. *Healthcare Sector*

Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services. December 2023. https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf
2. U.S. Department of Health and Human Services. HHS announces next steps in ongoing work to enhance cybersecurity for health care and public health sectors. Dec. 6, 2023. https://www.hhs.gov/about/news/2023/12/06/hhs-announces-next-steps-ongoing-work-enhance-cybersecurity-health-care-public-health-sectors.html

SOURCES

- **Jolie Apicella**, JD, Partner, Wiggin and Dana, New York City. Phone: (212) 551-2844. Email: japicella@wiggin.com.
- **William P. Dillon**, JD, Shareholder, Gunster, Tallahassee, FL. Phone: (850) 521-1708. Email: wdillon@gunster.com.
- **Jason Johnson**, JD, Partner, Crowell & Moring, New York City. Phone: (212) 520-1860. Email: jjohnson@crowell.com.
- **Kirsten Mickelson**, Cyber Practice Group Leader, Gallagher Bassett, Rolling Meadows, IL. Phone: (630) 773-3800.
- **Iliana L. Peters**, JD, Shareholder, Polsinelli, Washington, DC. Phone: (202) 626-8327. Email: ipeters@polsinelli.com.

Hospital Crippled by Days-Long Cyberattack

Lurie Children's Hospital, Chicago's largest pediatric provider, experienced a cyberattack that crippled its email systems and most of its phone service for nearly two weeks. The hospital's Epic MyChart system remained offline after most services were restored, requiring patients, families, and community providers to instead use a call center the hospital launched after the attack.

The Rhysida ransomware group reportedly claimed responsibility for the cyberattack and listed the hospital's data for sale on a dark web site for $3.4 million, but the hospital did not confirm those reports.[1]

The Chicago incident highlights the need for healthcare organizations to take steps that can mitigate risk up front before something goes wrong, says **Donald DePass**, JD, an attorney with Hogan Lovells in Washington, DC. Organizations can enforce data minimization and retention practices that limit the information they maintain that could be exposed in an incident, he says. That includes limiting the amount of personal information collected to what is necessary for them to provide their products and services to their customers and their patients.

"The idea is restricting the footprint and limiting the number of places that the data resides and potentially could be subject to unauthorized access or use," DePass says. "Another step organizations can take to mitigate risk up front is just educating their workforces on the protections that they have in place to safeguard data [and] training on privacy and security policies."

It also is important to promptly apply software updates and patches, use tools like multifactor authentication and encryption, regularly back up important data, and regularly evaluate the effectiveness of security controls to identify potential risks and vulnerabilities, DePass says.

"Organizations would be wise to make sure that their vendors are taking similar actions. Often, when a healthcare organization experiences an incident that impacts its data, the incident actually originates from a vendor or service provider that they've entrusted with their sensitive data," he says. "It would be prudent to confirm that those vendors are also taking appropriate actions to protect the data." ■

REFERENCE

1. Gallardo M. Lurie Children's Hospital restores key systems more than month after cyberattack. ABC7 Chicago. March 5, 2024. https://abc7chicago.com/lurie-childrens-hospital-chicago-new-my-chart-cyberattack/14492465/

SOURCE

- **Donald DePass**, JD, Hogan Lovells, Washington, DC. Phone: (202) 637-3286. Email: donald.depass@hoganlovells.com.

COMING IN FUTURE MONTHS

- Trends in medical malpractice claims
- Addressing compassion fatigue
- Hot topics in compliance
- Are HIPAA audits returning?