ISSUE 234 • 3RD QUARTER 2026

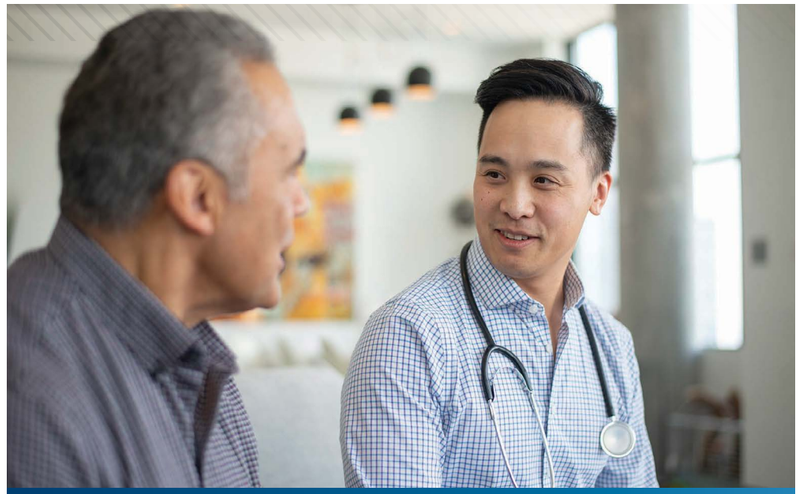
copiscope

INSIDE THIS ISSUE...

copic

www.copic.com

copiscope | Here for the Humans of Healthcare



Copiscope Editorial Committee

Our *Copiscope* Editorial Committee consists of Copic physicians, attorneys, insurance experts, and public affairs professionals as well as physician advisors, partners, and consultants. They work together to develop each issue of the newsletter and focus on addressing current issues in healthcare that are relevant to the medical providers and professionals we insure.

Have a question or suggestion for a future article for *Copiscope*? Please email rpeacock@copic.com.

COPIC CHECKUP:

Reminders & Updates

2026 Deadline to Earn Copic Points for a Premium Discount is 10/31

The Copic Points Program is designed to support your practice with valuable educational and risk mitigation resources and it provides the opportunity to earn a 10% discount for eligible insureds. The current cycle ends October 31, 2026.

Program Highlights:

- Earn CME/ CNE and Copic points through participation
- New Copic insureds automatically receive the discount in their first year; participation is required in subsequent years.

Ways to Earn Copic Points:

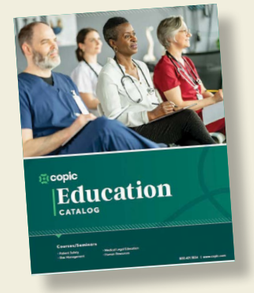
- **On-demand courses:** Earn points on your own schedule with 70+ topics including specialty-specific trends, managing unanticipated outcomes, patient communications, and interactive case studies. Access on-demand courses at www.copic.com/education.
- **Bite-Size Webinar:** An educational series that explores trending topics in healthcare.
- **Mock Trials:** Get a glimpse into courtroom proceedings during a medical liability trial.
- **Safety and Risk Strategy Assessments:** Managed by specially trained nurses, Copic's assessments offer an objective review based on evidence-based guidelines.
- **Rural Obstetrics Consortium:** A virtual presentation designed for OB leaders and risk management staff.
- **3Rs Program Training:** Copic's 3Rs Program (Recognize, Respond, and Resolve) is an early intervention program, separate and apart from their provider's insurance, to assist patients with out-of-pocket medical expenses when the outcome is not what the patient and the healthcare team expected.
- **Collaborative Plans:** If your group is participating in a Collaborative Plan, your education program is tailored for you and there is no need to participate separately in the above noted activities.

Check out our Copic activities on page 18 for a list of upcoming opportunities. If you need help creating an account to access our on-demand education offerings, please contact us at 720.858.6160 or email CustomerSupport@copic.com for assistance. If you have questions about the Copic Points Program, reach out to our Patient Safety and Risk Management department at grkm@copic.com, or visit our website: www.copic.com/copic-points-program.

Thank you for your continued commitment to patient safety.

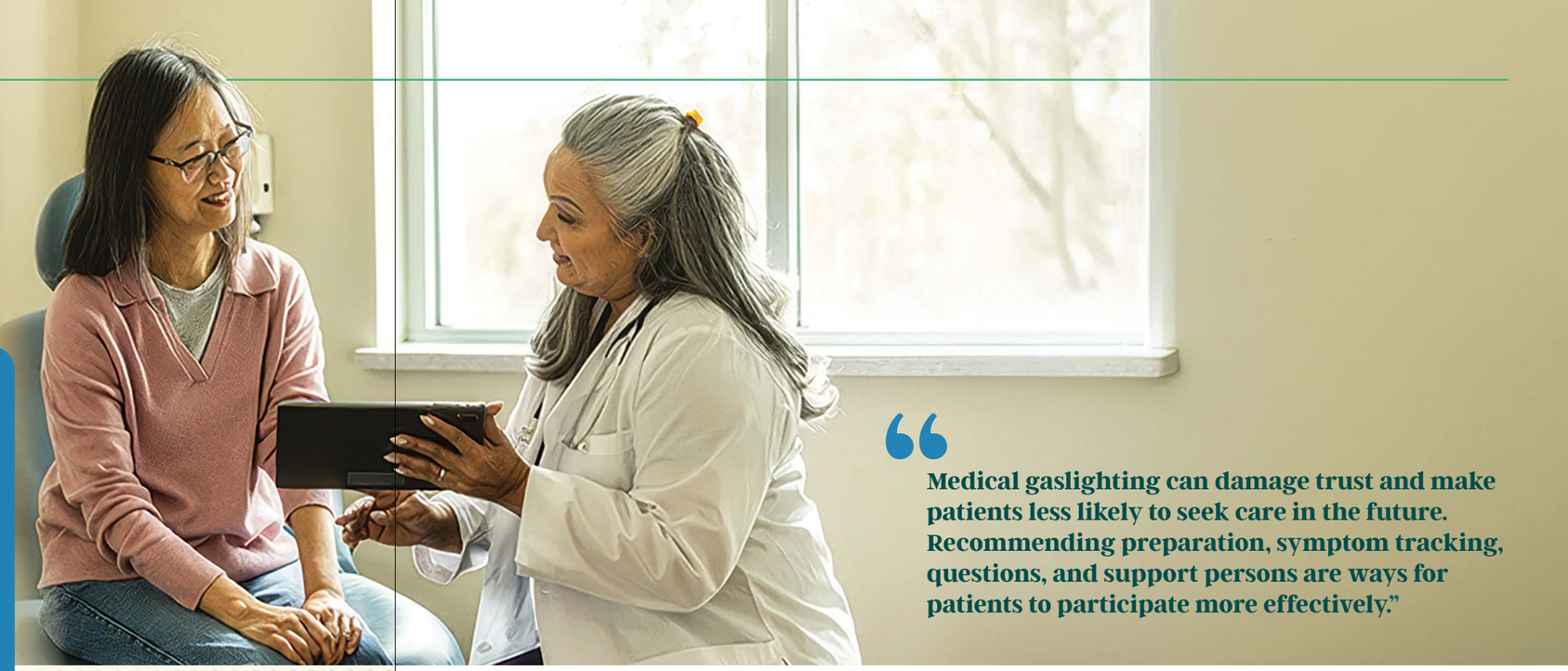
Did You Know?

Copic offers more than **50** live courses to our insureds. This is a benefit that comes with your policy: *there's no extra cost to you.* Our physicians, nurses, attorneys, and other team members share information on key patient safety issues, legal topics based on our experience and sharing our takeaways from de-identified closed claims. Some seminars can even be customized to your organization.



You can find our 2026 Education Catalog, including a list of Popular Courses on our website here: www.copic.com/education. For more information or to schedule a presentation reach out to Carmenlita Byrd at cbyrd@copic.com.

Medical Gaslighting: Listening as a Patient Safety Strategy



Most physicians do not enter an exam room intending to dismiss a patient's concern. In fact, the opposite is usually true: clinicians are trying to solve complex problems under time pressure, with incomplete information, administrative demands, and the cognitive shortcuts required to move through a busy clinical day. But even when unintentional, dismissing or minimizing a patient's symptoms can have serious consequences like missed diagnoses, delayed treatment, avoidable harm, and erosion of trust.

That is why "medical gaslighting" has become an important patient safety concept. In a recent episode of Copic's *Within Normal Limits* podcast, Dr. Eric Zacharias and Dr. Susan Sgambati describe medical gaslighting as the invalidation of a patient's genuine concerns without appropriate evaluation or investigation, not as deliberate manipulation, but more often as an unconscious cognitive and systemic phenomenon.

The American Journal of Medicine[1] similarly defines medical gaslighting as the inappropriate dismissal or invalidation of clinical concerns, while noting that the term can be overused when applied to any disagreement or difficult clinical interaction.

WHY THIS MATTERS NOW

In 2025, ECRI[2] named "risks of dismissing patient, family, and caregiver concerns" as a top patient safety concern of the year. ECRI noted that time constraints, resource limitations, communication challenges, and clinician bias can contribute to missed or delayed diagnoses when patient concerns are not fully heard. ECRI also emphasized that these events are often products of the systems in which clinicians and patients operate, not simply isolated failures by individual physicians.

The connection to diagnostic error is especially important. The National Academies' landmark report *Improving Diagnosis in Health Care*[3] defines diagnostic error as the failure to establish an accurate and timely explanation of the patient's health problem or to communicate that explanation to the patient.

Recent research underscores the scale of the problem. A 2024 diagnostic safety primer from AHRQ PSNet[4] notes that diagnostic errors remain a major patient safety issue and that cognitive shortcuts—while often necessary and useful—can contribute to errors such as anchoring, premature closure, availability bias, and overreliance on test results.

> **"Medical gaslighting can damage trust and make patients less likely to seek care in the future. Recommending preparation, symptom tracking, questions, and support persons are ways for patients to participate more effectively."**

WHEN "EFFICIENT THINKING" BECOMES A RISK

Physicians rely on mental shortcuts to practice efficiently. Pattern recognition is often a clinical strength: chest pain plus diaphoresis raises concern for acute coronary syndrome; fever during respiratory virus season may reasonably suggest a viral illness. But, these shortcuts can become vulnerable to error when they harden into assumptions.

Common cognitive traps include:

- **Premature closure:** stopping the diagnostic process once a "good enough" answer appears.
- **Availability bias**: overestimating a diagnosis because it has been seen repeatedly or recently.
- **Anchoring:** holding onto an initial impression despite new or discordant information.
- **Framing effects:** allowing contextual cues such as prior labels, behavioral history, weight, age, or mental health diagnoses to shape interpretation of symptoms.

These same biases are well-recognized in diagnostic error literature. AHRQ PSNet describes how heuristics can lead clinicians to miss atypical presentations or coexisting conditions, especially when time pressure and incomplete information are present. In the podcast, Dr. Zacharias offers a practical example: chest symptoms may trigger an ACS workup, but a normal troponin should not prematurely close the door on other high-risk diagnoses such as dissection, pulmonary embolism, or pericarditis.

LANGUAGE THAT CLOSES DOORS— AND LANGUAGE THAT OPENS THEM

Medical gaslighting often shows up in communication before it shows up in the chart. The podcast highlights "never words"—phrases that may feel efficient to the clinician but can shut down dialogue for the patient. Examples include: "You need to be realistic," "It's just part of the disease process," "I already explained this," "Let's not worry about that now," or "I've been doing this for 20 years."

These phrases can unintentionally communicate that the patient's experience is not credible or worth further exploration. A more productive approach is to validate the concern without overpromising certainty:

- *"Your symptoms are real, and I want to understand what we may be missing."*
- *"The tests we have so far have not shown a cause, but that does not mean nothing is going on."*
- *"Let's step back and revisit the timeline."*
- *"Here is what would make me want you to call, return, or go to the emergency department."*

This kind of language supports diagnostic humility. It also protects the therapeutic relationship. Harvard Health[5] notes that medical gaslighting can damage trust and make patients less likely to seek care in the future, while recommending preparation, symptom tracking, questions, and support persons as ways for patients to participate more effectively. For physicians, the parallel obligation is to create clinical space where that participation is welcomed.

Medical Gaslighting: Listening as a Patient Safety Strategy (from page 5)

> When symptoms are persistent, atypical, or multisystemic, consider referral, curbside consultation, or team-based review."

Practical Takeaways for Clinicians

1. **Pause when the story does not fit.** A return visit, persistent symptoms, new neurologic findings, escalating pain, or a patient saying "this feels different" should trigger a diagnostic pause. The goal is not to order every test—it is to deliberately reconsider the working diagnosis.
2. **Use "diagnostic time-outs."** Ask: What else could this be? What diagnosis would be dangerous to miss? What data does not fit? What am I assuming about this patient? These questions help shift from fast, intuitive reasoning to slower, more analytical thinking when uncertainty is high.
3. **Document the patient's words.** Dr. Sgambati recommends capturing the patient's exact words before translating them into clinician interpretation. This can reduce bias in the record and preserve clues that may matter later.
4. **Avoid labels that undermine credibility.** Terms such as "complainer," "dramatic," or "difficult" can follow patients through the chart and shape future care. If behavior is clinically relevant, document objective observations and the clinical response.
5. **Normalize uncertainty.** Saying "I don't know yet" is not a failure. It can be a sign of careful medicine—especially when paired with a plan, follow-up, safety net instructions, and shared decision making.
6. **Bring in help early.** When symptoms are persistent, atypical, or multisystemic, consider referral, curbside consultation, or team-based review. As the podcast notes, calling a colleague and saying, "I'm struggling with this case. Can I walk you through it?" can be both clinically useful and professionally grounding.

Summary

Medical gaslighting is not just a communication issue; it is a patient safety issue. It sits at the intersection of diagnostic reasoning, trust, bias, documentation, and system design. The solution is not to abandon clinical judgment or treat every patient concern as equally probable. Rather, it is to remain curious when the clinical picture is incomplete, to recognize when cognitive shortcuts may be narrowing the differential, and to communicate in ways that preserve the patient's role as a partner in diagnosis.

[1] https://www.amjmed.com/article/S0002-9343%2824%2900396-6/fulltext

[2] https://home.ecri.org/blogs/ecri-thought-leadership-resources/top-10-patient-safety-concerns-2025

[3] https://nap.nationalacademies.org/reso urce/21794/interactive/

[4] https://psnet.ahrq.gov/primer/diagnostic-errors

[5] https://www.health.harvard.edu/healthy-aging-and-longevity/what-to-do-about-medical-gaslighting

SPECIALTY FOCUS

Internal Medicine/ Family Medicine

A Guide to Addressing Common Areas of Risk

	Key Areas for Errors	Strategies to Reduce Errors
Failure to Diagnose or Delayed Diagnosis	• **Heads—acute neurological presentations:** CVA, SAH, epidurals, encephalitis/meningitis and space occupying spinal cord lesions • **Hearts—chest pain triple rule-out:** MI/ACS, PE, dissection • **Guts—acute abdominal emergencies:** appendicitis, perforations, ischemic bowel, abscess • **Bugs—severe infectious diseases:** sepsis, necrotizing fascitis, MRSA, SBE, septic joints	• **Recognize the narrow window of opportunity** to make these rare but serious diagnoses • **Perform a good exam and document it,** including neurologic when appropriate • **Use imaging and communicate** with your radiologist • **Urgent consults**—you own the window of time until your patient gets there • **Vital signs are important,** especially trends and discharge vitals • **Document** what you are thinking
Cancer	• **Timely diagnosis** of and screening for breast, colorectal, lung, melanoma and prostate malignancies • **Incidental findings on imaging** warrants work-up or follow-up imaging	• **Sophisticated tickler and tracking systems** • **Risk-specific screenings** and document their completion or refusal • **Systematic work-up** of symptomatic findings • Once there is an incidental finding, **track it through the process** • **Alert patient** of any findings, recommendations, and document in the chart • **Use closed loop communication** to alert any other providers who may need to know about the findings
Medication Errors	• Dosing errors • Look alike/sound alike medications • Allergies or adverse drug reactions • Failure to monitor	• **Ensure the right prescription, right delivery, and right dose;** understand how your electronic systems can help or hinder this • **Proper patient education and monitoring**

Copic Resources

3Rs Program: Early intervention and resolution program to preserve relationships

24/7 Risk Management Hotline: Physician risk managers available for guidance

Education: Specialty-specific education, on-demand courses, virtual programs, and seminars

Online Resource Center: Consent forms, practice management resources, an archive of past newsletters, and more

Ask ECRI: High-Risk Electronic Communication Behavior

This is part of the "Ask ECRI" series of articles provided to Copic to share with our insureds; it focuses on questions ECRI receives from members regarding healthcare issues and concerns. ECRI is an independent, nonprofit organization improving the safety, quality, and cost-effectiveness of care across all healthcare settings.

Electronic communication in healthcare continues to simultaneously support accessible communication among providers and patients and serve as a source of significant liability when that communication fails. Advances in communication technologies such as electronic health record (EHR)-based secure chats, secure texting platforms (STPs), other internal messaging systems, and patient portals have all strengthened certain aspects of communication with positive effects on patient safety. However, they have also introduced new risks that can result in both patient and system harm, especially when they are not thoughtfully implemented or governed with clear policies, training, and oversight.

SCOPE OF BENEFIT AND RISK

INTERPROFESSIONAL COMMUNICATION

The use of EHR-based secure messaging such as Epic Secure Chat and Cerner CareAware is rapidly increasing. For example, though usage often varies across clinical roles and work contexts, one study[1] found a 29% increase in weekly message volume over a six-month period across 14 hospitals and more than 260 outpatient clinics. While research suggests this technology has become the preferred method of interprofessional communication due to its ease of use, integration with clinical workflows and patient charts, and flexible response expectations (i.e., prioritization of messages), questions about whether it actually improves communication have been raised.

Surveys of clinicians from an academic medical center[2], a quaternary care children's hospital[3], and an academic safety net hospital system[4] note positive perceptions about the technology's support of teamwork, including:

- Multiple communication modalities and technological features
- Increased interprofessional communication that is easily accessible, rapid, and reliable
- Relationship building
- Interdisciplinary care coordination

However, several risks were also identified, such as:

- Inappropriate use for urgent communication
- Decreased or delayed frontline decision making
- Lack of closed-loop communication practices
- Increased workload and cognitive burden or stress related to communication volume
- Workflow inefficiencies (e.g., alarm/notification fatigue, interruptions to clinical work, miscommunication)
- Decreased face-to-face communication that risks loss of nuance

Moreover, increased use of secure messaging has been associated with increased telephone usage[5], suggesting that novel communication channels may not mitigate the use of existing or traditional channels, thereby increasing the overall burden of communication.

PROFESSIONALISM

Electronic communication inherently lends itself to embodying a casual style that may be interpreted as unprofessional. It lacks the visual and auditory cues that face-to-face interactions provide and obscures the intended tone. Responding rapidly or neglecting to review the message prior to sending can leave inaccurate autocorrections, typos, and other errors that may result in misunderstandings.

Modern texting often involves loose adherence to traditional grammar rules indicative of informal conversation (e.g., lack of punctuation, proper sentence structure, use of emojis or GIFs) and can blur the lines of professional boundaries. While using modern texting lingo may be an unspoken, acceptable "non-best practice" among colleagues or even patients, it does not—and should not—circumvent the obligation to uphold professional standards and boundaries expected of healthcare providers.

Research on secure message content is modest but suggests that professionalism is maintained. A study of messages among hospitalists[6] found that most "focused on clinical management of patient needs (62%) and functioned to provide a notification or update regarding clinical care (64%) or make a request of the recipient (63%)" (e.g., patient symptoms, physician orders, medications, procedures, care transitions). Only 10% of messages contained personal content, and almost all remained "professional in nature and work related," such as using emojis to soften work-related requests or celebrating birthdays.

RETENTION REQUIREMENTS

The Centers for Medicare & Medicaid Services (CMS)[7] allows texting patient information and orders among providers through a HIPAA-compliant STP and requires medical records to be retained for at least five years[8].

HIPAA requires covered entities and business associates to securely store and retain HIPAA-related documentation for six years, yet defers to state law for medical record retention requirements that vary from the CMS minimum of five years.

Organizations should consult their legal counsel and compliance officers for appropriate retention policies regarding secure messaging, whether through the EHR system or a stand-alone platform.

BEST PRACTICES

Other resources that may prove helpful in developing policies and procedures or informing quality improvement initiatives for secure messaging include the following:

- American College of Physicians Ethical Guidance for Electronic Patient-Physician Communication: Aligning Expectations (Journal of General Internal Medicine)
- American Medical Association STEPS Forward modules:
  - Patient Portal Optimization: Engage Patients While Minimizing Care Team Burden
  - A Systematic Approach to Reducing EHR Inbox Burden
- Digital Professionalism: Maintaining Professional Standards When Using Digital Messaging Platforms (Nursing Standard)
- Patient Electronic Messaging: 12 Tips to Save Time (American Academy of Family Physicians)

Quick Click:
Scan to access clickable links to these resources.

[1] https://www.jmir.org/2023/1/e48583

[2] https://journals.lww.com/qmhcjournal/abstract/9900/navigating_communication__crafting_guidelines_for.146.aspx

[3] https://shmpublications.onlinelibrary.wiley.com/doi/10.1002/jhm.12953

[4] https://link.springer.com/article/10.1007/s10916-023-01956-x

[5] https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2820225

[6] https://bmjopenquality.bmj.com/content/12/3/e002385

[7] https://www.cms.gov/files/document/qso-24-05-hospital-cah.pdf

[8] https://www.ecfr.gov/current/title-42/chapter-IV/subchapter-G/part-482/subpart-C/section-482.24

When Law Enforcement Requests Patient Information:

Practical Guidance for Physicians

Interactions with law enforcement can place physicians and healthcare teams in a difficult position: wanting to cooperate with public safety officials while also protecting patient privacy, complying with HIPAA, and preserving trust in the physician-patient relationship. The default rule under HIPAA is that protected health information, or PHI, should not be disclosed without the patient's authorization unless a specific exception applies, such as a disclosure required by law or certain law enforcement-related circumstances.

The key is not to treat every law enforcement request the same. A police officer asking a question in a hallway, a detective presenting a subpoena, a sheriff's deputy accompanying a patient in custody, and an officer requesting information during an emergency may all raise different legal and operational considerations. HIPAA permits certain disclosures to law enforcement without patient authorization, but those permissions are limited and fact-specific.

Start with the basics: Is this PHI?

Before disclosing patient information to law enforcement, a provider should consider whether it is protected under the federal Health Insurance Portability and Accountability Act (HIPAA) rules, which provide privacy protections for individually identifiable health information held by healthcare clinicians and their business associates. HIPAA "covered entities" include healthcare clinicians who transmit any health information in electronic form in connection with a transaction covered under the HIPAA regulations.

Protected health information (PHI) includes individually identifiable health information transmitted or maintained in electronic media or any other form or medium.

Individually identifiable health information is information created or received by a healthcare clinician that identifies the individual and relates to the past, present, or future physical/mental health or condition of an individual; the provision of healthcare to the individual; or payment for the provision of healthcare to the individual.[1]

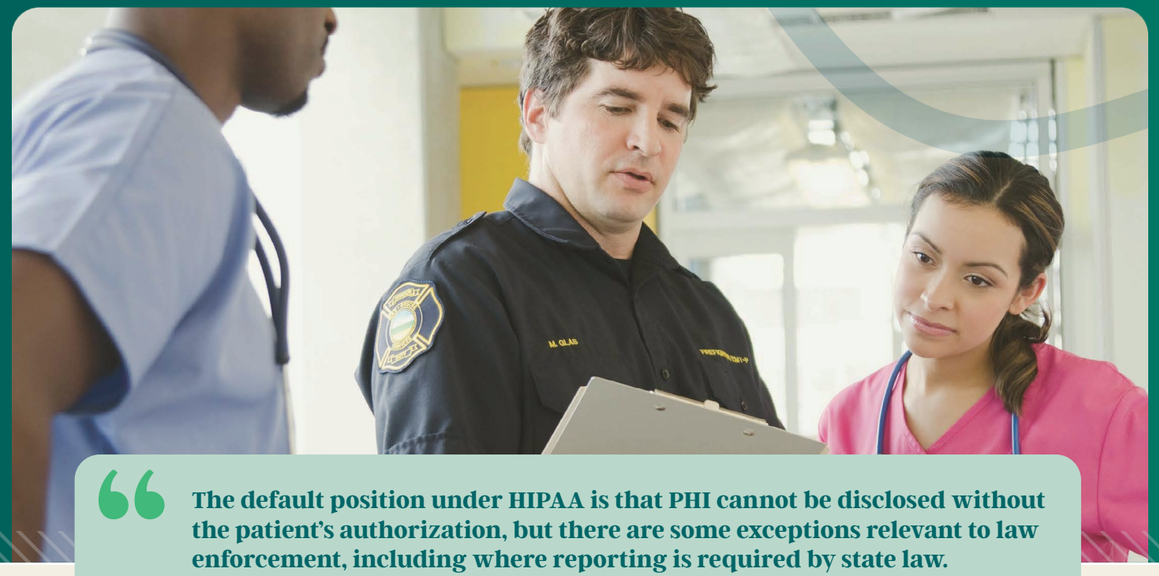
Who Is Considered a Law Enforcement Official?

As outlined in the HIPAA Privacy Rule, a law enforcement official means an officer or employee of any agency or authority within the U.S., who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.[2]

Law enforcement officials include (but are not limited to):

- Police officers and state troopers
- Sheriffs and sheriffs' deputies
- District attorneys
- DEA and FBI special agents
- ICE officers



> **The default position under HIPAA is that PHI cannot be disclosed without the patient's authorization, but there are some exceptions relevant to law enforcement, including where reporting is required by state law.**

Key Considerations for Any Law Enforcement Interaction:

Don't be afraid to ask for identification. Have they properly identified themselves? If the law enforcement official is not known to the clinician, the clinician must verify the identity and authority of the person.[3] Processes should be in place for in-person, phone, and email interactions.

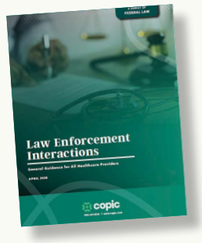
Share your side of the situation. Explain your understanding of the situation and the laws (HIPAA, etc.) that govern your actions of what you can and can't do.

When trying to decide which federal or state law applies, the more restrictive one will likely apply. In general, if there is a state or federal law that is more restrictive than HIPAA (more protective of a patient's privacy), clinicians are required to comply with the more restrictive law.

Document the details. Carefully document any disclosures and any supporting information about why the decision was made to provide information to law enforcement officials.[4]

Respect law enforcement and the challenges they are dealing with. Do not physically interfere with law enforcement officials or provide them false or misleading information.

Don't provide more information than what is necessary. Unless disclosures made to law enforcement are required by law, they should be held to the "minimum necessary" standard. This means that when using or disclosing protected health information (PHI), the HIPAA-covered entity or clinician must make reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose of the use, disclosure, or request.[5] A clinician may rely upon the representations of a law enforcement official that the information requested is the minimum necessary for the stated purpose.[6]



For more information about the responsibility to patients while respecting the requests of law enforcement, download a copy of our resource booklet, ***Law Enforcement Interactions***, available at www.copic.com/tools-and-resources.

You will need to be logged in with your username and password to access this resource.

[1] 45 C.F.R. § 160.103
[2] 45 C.F.R. § 164.103
[3] 45 C.F.R. § 164.514(h)(1)(i)
[4] 45 C.F.R. § 164.514(h)(1)(ii)
[5] 45 C.F.R. § 164.502(b)
[6] 45 C.F.R. § 164.514(d)(3)(iii)(A)

Awareness of Insider Threats

While many cybersecurity threats come from external attackers, insider threats can be just as damaging. Insider threats involve individuals within an organization who misuse their access to compromise systems, steal data, or cause disruptions. Whether intentional or accidental, insider threats pose a significant risk to businesses. This guide explains what insider threats are, why they matter, and how you can recognize and mitigate them.

What Are Insider Threats?

An insider threat occurs when someone within an organization—such as an employee, contractor, or partner—misuses their access to compromise security. These threats can be categorized as:

1. **Malicious Insiders:** Individuals who intentionally harm the organization, often motivated by financial gain, revenge, or external influence.
2. **Negligent Insiders:** Employees who accidentally expose data or compromise systems through carelessness or lack of awareness.
3. **Third-Party Insiders:** Contractors, vendors, or partners with access to the organization's systems who unintentionally or deliberately pose a security risk.

Why Insider Threats Matter

1. **Access to Sensitive Information:** Insiders often have legitimate access to critical systems and data, making it easier to cause harm.
2. **Difficult to Detect:** Insider threats can blend in with normal activities, making them harder to identify than external attacks.
3. **Significant Impact:** Insider threats can lead to financial loss, reputational damage, and regulatory penalties.
4. **Growing Risks:** Remote work, cloud services, and increased data sharing have expanded the potential for insider threats.

Examples of Insider Threats

- **Data Theft:** An employee downloads sensitive customer data before resigning.
- **Unauthorized Sharing:** A contractor shares proprietary information with a competitor.
- **Negligent Actions:** An employee clicks on a phishing link, granting attackers access to company systems.
- **Sabotage:** A disgruntled employee intentionally deletes important files or disrupts systems.

Recognizing Insider Threats

BEHAVIORAL INDICATORS

- Sudden changes in behavior, such as withdrawing from colleagues or expressing dissatisfaction with the organization.
- Unexplained attempts to access systems or data not relevant to their role.
- Excessive downloads or transfers of sensitive files.
- Frequent policy violations, such as ignoring security protocols or bypassing controls.

TECHNICAL INDICATORS

- Accessing systems outside of normal working hours without a legitimate reason.
- Multiple failed login attempts or use of shared accounts.
- Unusual data transfers to personal devices, external drives, or unauthorized cloud services.

How to Mitigate Insider Threats

1. **Follow Access Control Policies**
   - Only access systems and data necessary for your role.
   - Avoid sharing login credentials or using shared accounts.
2. **Report Suspicious Activity**
   - Notify your IT or security team if you observe unusual behavior, such as excessive data transfers or attempts to bypass security measures.
3. **Adhere to Security Protocols**
   - Follow organizational policies for handling sensitive data, such as encryption and secure file sharing.
   - Avoid disabling security features, like firewalls or antivirus software, on work devices.
4. **Participate in Training**
   - Attend regular cybersecurity training to understand insider threats and how to recognize them.
   - Stay informed about emerging risks and best practices.
5. **Protect Against Negligence**
   - Be cautious when clicking on links or downloading attachments, especially from unknown sources.
   - Secure your devices with strong passwords and lock screens when not in use.

What to Do If You Suspect an Insider Threat

1. **Document Observations:** Take note of unusual behavior or activities and gather evidence if possible (e.g., timestamps, file names).
2. **Report Concerns Immediately:** Contact your manager or the IT/security team to escalate the issue. Avoid confronting the individual directly.
3. **Avoid Assumptions:** Not all unusual behavior is malicious. Reporting concerns to the appropriate team ensures a fair and professional investigation.

The Role of the Organization

While employees play a critical role in detecting and mitigating insider threats, organizations are responsible for implementing robust defenses, including:

- **Monitoring and Logging:** Tracking access and activities to detect unusual patterns.
- **Role-Based Access Controls:** Restricting access to sensitive data based on job responsibilities.
- **Regular Audits:** Conducting routine checks on system usage and compliance.
- **Awareness Campaigns:** Providing ongoing training to educate employees about insider threats.

Summary

Insider threats pose a significant risk to organizations, but awareness and proactive measures can help mitigate them. By following security protocols, staying vigilant, and reporting suspicious activities, employees can play an essential role in protecting their organization from both intentional and accidental insider threats.

Remember, cybersecurity is a shared responsibility that starts with you.

Copic 101

When Part-Time Insurance Coverage May Make Sense

Copic recognizes that not every physician's practice follows a traditional full-time schedule. As practice patterns change, some physicians reduce their hours as they transition toward retirement, return from leave, build a new practice, provide occasional coverage, or volunteer on a limited basis. For eligible insureds, Copic's part-time credits may help align premium costs with a physician's actual clinical exposure.

5 Real-Life Situations Where Part-Time Coverage May Apply

1. **EASING INTO RETIREMENT**
   A physician may want to continue practicing while reducing their schedule to one or two days per week.

2. **STARTING A NEW PRIVATE PRACTICE**
   A physician may initially see patients only a few days per week while building referral relationships, hiring staff, finalizing payer contracts, or establishing operations.

3. **RETURNING AFTER LEAVE OR A SABBATICAL**
   Some physicians gradually resume practice after parental leave, caregiving responsibilities, a sabbatical, or another personal transition.

4. **PROVIDING OCCASIONAL LOCUM TENENS OR MOONLIGHTING SERVICES**
   A physician with a full-time administrative, academic, or non-clinical role may occasionally provide clinical coverage. Depending on the work arrangement, individual coverage may be needed, or the physician may need to confirm that coverage is provided by the hiring organization.

5. **VOLUNTEERING OR WORKING IN A LOW-VOLUME CLINIC**
   A physician may volunteer at a community clinic, provide care at a health fair, or serve in a charitable medical setting. Even when compensation is minimal or not provided, liability exposure may still exist.

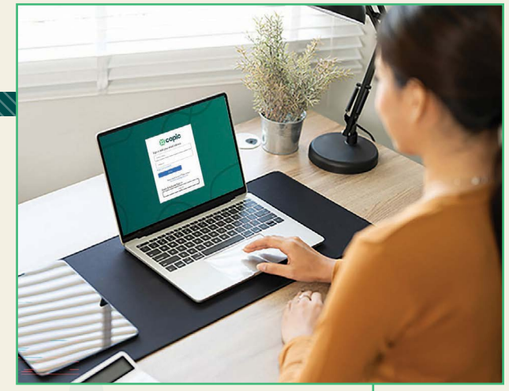
Copic offers part-time discounts for insureds who average fewer than 26 hours of practice per week. When calculating hours, include patient care, charting, rounding, and actual on-call patient care activities. Hours should be averaged over at least one quarter to reflect a consistent practice pattern. If your schedule has changed or you are regularly working fewer hours, it may be a good time to check whether you qualify for a part-time credit.

Contact Copic to Discuss Your Options

For physicians considering part-time practice, please contact your Copic underwriter to discuss the options available. You can find your underwriter on www.copic.com within the Customer Portal after you log in with your username and password. You can also call Copic Customer Support at 720.858.6160 or email us at customersupport@copic.com.

Communication Preferences:

Updated Features in the Customer Portal Help Manage Account Access



The Customer Portal on Copic's website now includes enhanced account management features that give policyholders more control over portal access, account contact roles, and communication preferences.

PORTAL ACCESS

Policyholders, account administrators, and agency administrators can now manage portal access directly, managing preferences like adding a new person to an account, granting existing portal users access to an additional account, updating a user's name, email, or access level, and removing access when it's no longer needed. *Please note: named insureds and policyholders are still managed through the policy system rather than the portal, so any changes to those records should continue to go through an assigned underwriter.*

CONTACT ROLES

Alongside portal access, accounts can now assign contact roles to the people associated with them. Contact roles define each person's responsibility or relationship to the account and determine which categories of Copic communications they're eligible to receive. Every person is assigned a default contact role automatically based on their account access, and administrators can add or remove additional eligible roles as responsibilities change.

COMMUNICATION PREFERENCES

Communication preferences build directly on contact roles. For each content category, such as newsletters, announcements, education, etc., administrators choose whether eligible users are opted in by default and whether each person is allowed to set their own individual preferences. *While users have greater flexibility to personalize communications, required policy, billing, and claims-related communications will continue to be delivered to ensure important information is received and compliance requirements are met.*

These improvements are designed to put more control in the hands of the people who know their organizations best, while keeping essential communications flowing without interruption. Contact Customer Support at customersupport@copic.com with any questions, or to receive an invitation to set up a portal account.

For step-by-step instructions on how to update your preferences and contact roles, reference our two new training guides available in the Customer Portal:

- **Customer Portal: User Management Guide**
- **Customer Portal Guide: Managing Contact Roles & Account-Level Communication Preferences**

> To access the training guides, log in to your Copic account by clicking the Customer Portal icon in the top-right corner of our homepage at copic.com. Navigate to the Preferences tab on the left and the guides can be found within the corresponding dropdown menus.

Legislative Landscape

Preparing for What's Ahead in 2027

As the dog days of summer have transitioned into back-to-school season, the Copic Public Affairs team is shifting our focus toward what the 2027 legislative session could have in store for us.

WHAT'S THE BIG PICTURE?

The 2026 primary elections are behind us. The primary election results indicated a shift toward change from the status quo. This is nothing we did not expect in a midterm election year.

In Colorado, we saw a shift from "establishment" incumbent legislators to self-proclaimed "anti-establishment" candidates. In Minnesota, we're seeing over 26 House members and 17 senators stepping down at the end of this year, which significantly changes the balance of the legislature next year. Gubernatorial primaries in Colorado and Iowa presented unexpected results, favoring what some viewed as the underdog candidates. And South Dakota's Republican gubernatorial primary went into a runoff, which Governor Larry Rhoden won in a landslide.

The Copic Public Affairs team is continuing to track developments leading up to the general elections on November 3, 2026.

What Has Copic Been Up To in the Interim?

ON THE POLITICAL SIDE...

We have been proactively engaging conversations with current and prospective legislators. We bring them up to speed on the need to protect access to quality care, preserve the physician-patient relationship, and maintain the ability to review and improve care. For first-time candidates running for office, these early conversations allow our team to identify candidates who are or may be aligned with the Copic mission. From there, we work to build trust and understanding on our issues.

ON THE POLICY SIDE...

The interim months are also utilized for proactive policy setting conversations. This year, the hot topic is med spa regulations. There are roughly 10,500 med spas that are operating across the country, according to the American Med Spa Association. And the American Medical Association highlighted that 36 states lack any specific laws or regulations written directly for these practices. The Copic team is engaging in conversations with legislators and stakeholder partners on how best to regulate these facilities to ensure patient safety and transparency in care.

What Can You Do to Engage?

As we consider the 2027 legislative session, we want to remind you that your voice as a healthcare clinician is valuable in the legislative process. We recommend that you start with the steps below.

- **Be curious**
  To start, you can look up your state legislators by entering your address on our "View Your Election Center" feature on the Healthcare Advocacy page (www.copic.com/healthcare-advocacy) on the Copic website. When it comes to tracking and engaging on policy issues across our core footprint, Copic's got you covered. However, we encourage you to ask us questions, engage through your state medical association, and testify on bills when your voice and your story are needed.
- **Understand your expertise and its value**
  As a clinician, you have expertise into the care and treatment of patients and the policies that impact the delivery of that care. ***While the federal government gets more attention in the news, most legislation that dictates healthcare access and delivery is made at the state level.*** That's where your impact can make a difference. When the time is right, your stories are invaluable in communicating with legislators. Some examples may include your experience juggling the administrative hurdles of running your own practice or delivering care to patients in the emergency room. Help us build the bench and let the Copic Public Affairs team know if you're interested in testifying on bills or corresponding with your legislator.
- **Maintain relationships with your state legislators**
  Healthcare clinicians are often perceived as leaders in the community, especially in rural areas. Your legislator may already be aware of your practice and would like to know more. Reach out and introduce yourself! That way, when an issue arises that could impact your practice, your legislator will recognize your impact. The Copic team would also be happy to coordinate a legislator tour of your facility so they can hear directly from you on the issues that you are facing.

Visit **Copic's Healthcare Advocacy** page at www.copic.com/healthcare-advocacy for more information on bills we tracked during the legislative session, to sign up for newsletter updates, or to find your elected officials. If you have any questions, please contact Copic's Director of Public Affairs, Sarah Meirose, at smeirose@copic.com.

Mark Your Calendars for Upcoming Copic Activities

BITE-SIZE WEBINARS

We chat monthly about hot topics in healthcare for facility risk managers, clinic leaders, hospital staff and other medical providers. Noon to 1pm (Mountain Time) via Zoom. Attendance earns the insured facility 1 Copic point. Email Cathi Pennetta at cpennetta@copic.com for registration information.

- **October 7:** Top Patient Safety Concerns: Risks, Trends, and Solutions
- **December 2:** Well-Being

MOCK TRIALS

These sessions offer a peek into courtroom proceedings during a medical liability trial as we present an actual trial. Eligible attendees receive 2 Copic points and 3 CME or 3 CNE credits. Contact Gina Rowland at growland@copic.com with questions.

- **September 17, 6-9pm in person at the Insights Conference in Eagan, MN**
- **October 13, 6-9pm MT (virtual)**

COPIC'S CONFERENCES

Addressing key topics in safety and risk management featuring nationally-recognized speakers.

- **Rural OB Consortium (Virtual):** November 12. Featuring best practices and time for open discussion about the challenges and solutions in rural obstetric care. Attendance earns the insured facility 1 Copic point. Email Cathi Pennetta at cpennetta@copic.com for registration information.
- **Copic Insights (In-Person):** Details will be emailed for these conferences.
  - September 18, Eagan, MN
  - September 29, Des Moines, IA

PRACTICE ADMINISTRATOR WEBINARS

Copic hosts webinars throughout the year designed for practice administrators and the challenges they face. Besides addressing important topics, they're a forum to discuss issues with colleagues and build your peer network. Webinars are held from noon to 1pm (Mountain Time). Attendance earns the insured facility 2 Copic points to 2 eligible providers. For more information, contact Wendi Utzinger at wutzinger@copic.com.

- **October 28:** Hot Topics from Patient Safety & Risk Management

SEAN GELSEY
Chief Claims Officer

> **"This work is ultimately about helping clinicians understand that they are not alone, that preparation matters, and that Copic is here to protect and support them through one of the hardest professional experiences they may face."**

What I've Learned

About Litigation, Insurance, and Claims Management

Sean Gelsey, MBA, Copic's Chief Claims Officer, brings more than 30 years of experience in litigation, insurance, and claims management, helping physicians, healthcare facilities and healthcare professionals navigate one of the most difficult experiences of their careers: a medical liability claim or lawsuit. From that vantage point, he has seen how fear, uncertainty, communication, preparation, and trust can shape not only the legal outcome, but also the personal experience of the clinician involved. Before joining Copic, he retired from the United States Air Force and worked as a senior claims professional specializing in complex medical claims.

If a patient issue comes up, contact Copic right away—it's one of the best ways to protect yourself. One common misconception is that a matter only needs to be reported once a lawsuit is filed or papers are served. In reality, early reporting gives Copic and the defense team the best opportunity to understand what happened, preserve the medical record, evaluate the facts, and provide guidance before the situation escalates. Waiting can make an already stressful situation harder to manage and difficult to recall facts around care provided.

A claim can make you feel isolated and overwhelmed, but physicians are not alone in the process. Being named in a lawsuit can feel deeply personal, and many physicians assume they are carrying the burden by themselves. The defense attorney is there to advocate for that clinician, and Copic's role is to stand with the insured throughout the process. Our goal is to help shoulder the weight of the matter and develop the strongest path forward as a team.

Talking medicine with other physicians is one thing. Explaining it to people outside medicine is another. Physicians are experts in clinical care, but depositions and trials call for a different style of communication. Acronyms, shorthand, and assumptions that work among colleagues may not resonate with attorneys, jurors, or patients. My advice is to slow down, speak in plain language, and confirm understanding. The goal is not to dilute the medicine, but to explain it in a way that is clear, credible, and accessible to people who are not immersed in clinical practice every day.

Preparation changes the way a physician shows up. Preparing for a deposition or trial should be approached much like preparing for an exam. Physicians need to understand the care they provided, the reasons behind their decisions, what the record reflects, and how to answer only the question asked. Clear, credible testimony is essential, as is the confidence to say, "I don't know," when that is the truthful answer. Preparation helps clinicians avoid speculation, unnecessary elaboration filling silence, and preventable complications.

The applicable standard of care depends on the medical setting's geography and characteristics. A recurring lesson is that cases should not all be judged against the resources of a large metropolitan medical center. Rural communities and urban hospitals may operate with very different capabilities, and that context matters. Defense teams help clinicians understand how the standard of care is evaluated in light of the clinician's specialty, the facts, location, available resources, and circumstances surrounding the care.

Trust and candor with the defense team are essential. Successful defense depends on timely, accurate, and complete information. Physicians may hesitate to share everything, especially when they are anxious or worried about how information will be used. But the defense team needs the full picture to help. Surprises during a deposition or trial can be damaging. Open communication helps the team evaluate the matter, prepare the physician, and avoid preventable missteps.

Documentation should be timely, accurate, and left intact. Strong documentation can be one of the most important tools in defending a claim or lawsuit. Document according to established protocols and never try to add to or alter the record after a claim or lawsuit arises. Good documentation helps explain what happened; late or incomplete documentation can create new challenges.

What gives me hope in this field is legislative progress and rising talent. I'm encouraged by courts upholding damage caps and by states pushing back against third-party litigation funding, both of which are important to protecting the practice of medicine. At the same time, as many experienced professionals move closer to the later stages of their careers, there is a meaningful opportunity to mentor younger attorneys and claims professionals. Sharing lessons learned and strengthening collaboration across defense teams is one of the most rewarding parts of my work and an important investment in the future.

7351 E. Lowry Blvd., Ste. 400, Denver, Colorado 80230

Visit us at copic.com

Our website offers a wealth of helpful resources, program highlights, and Copic insight—all designed to help you succeed.

Copic Insurance Company

Switchboard
720.858.6000 or 800.421.1834

24/7 Risk Mgmt. Hotline
(for urgent, after hours inquiries)
866.274.7511

To Make an Incident Report
720.858.6395

Customer Support
720.858.6160

Copic Financial

720.858.6280

Website
www.copicfinancial.com

Copic Medical Foundation

720.858.6060

Website
www.copicfoundation.org