Ann & Robert H. Lurie
Children's Hospital of Chicago™
Children's Community Physicians Association

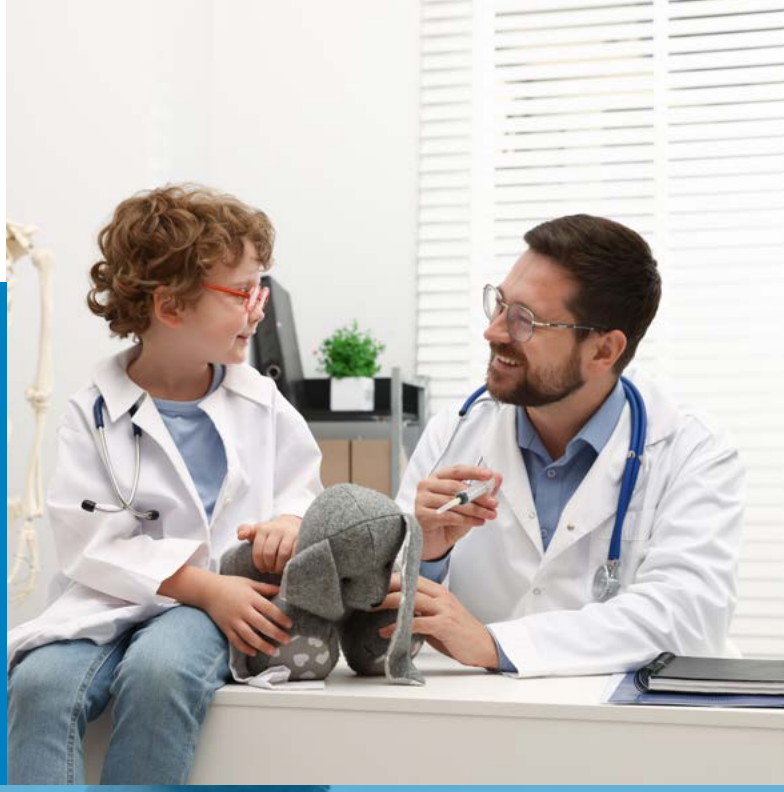


TABLE OF CONTENTS:

ccpa news

SUMMER/FALL 2026

Letter from CCPA/CCPAPP's Board President Jonathan Necheles, MD

According to an article in the Mayo Clinic Magazine, *The Rise of AI In Healthcare*, artificial intelligence (AI) has been a part of healthcare technology since the 1970's. And it has expanded more recently because of numerous technological advancements, specifically in the computerization of patient data via electronic health records (EHR), electronic claims submissions, telemedicine, and the use of AI ambient scribe tools (Kula, 2026). However, the key component in all this technology gain is that patients' data are now digitally stored and ready for AI to analyze and allow clinicians to provide faster and better care for their patients.

The article continued to state that there are three benefits of using AI in healthcare. The first benefit of AI is enhancing human knowledge by analyzing the patient's records for patterns and recommending treatment plans based on those findings. The second benefit is reducing clinicians' administrative tasks, such as note taking during the patient visit using ambient AI listening devices. Allowing the physician the opportunity to focus on the patient rather than on documentation. Lastly, incorporating AI into the clinical process, which leads to quicker diagnoses and creation of new treatment plans. Even with these benefits, AI still requires human oversight, review, and application.

Therefore, as AI usage continues to expand in healthcare, it is important that medical practices understand both its opportunities to simplify workflow as well as their responsibilities to monitor its usage. In this edition of CCPA News, we feature articles on establishing AI governance within your practice and how the Health Insurance Portability and Accountability Act (HIPPA) will affect AI usage. The goal is to provide CCPA members with a starting point for creating AI governance, and to help members adapt to this rapidly evolving technology, while maintaining their commitment to safe and efficient patient care.

References

Kula, S. (2026, April). The Rise of AI In Healthcare. Retrieved from Mayo Clinic Magazine: https://mayomagazine.mayoclinic.org/2026/04/ai-in-healthcare/

In the Spotlight

Did you know that CCPA has several members who are pediatric specialists? This section will provide a rotating spotlight on CCPA's subspecialists.

Diane L. Ozog, MD

Dr. Diane L. Ozog & Associates
1288 Rickert Drive, Suite 100
Naperville, IL 60540
630.625.0606 | www.drdianeozog.com

Diane L. Ozog, MD began her career in healthcare as a pharmacist and established her medical practice in the western suburbs of Chicago. For over 35 years, Dr. Ozog has specialized in providing treatment for asthma, allergies, and clinical immunology for patients of all ages. Dr. Ozog and her staff strongly emphasize the philosophy of educating their patients so that they can participate in their medical care by actively maintaining a healthy state of body and mind. This patient-centered approach encourages individuals to take an active role in managing their health through knowledge and support.

Diane L. Ozog, MD

Dr. Ozog graduated with honors from the University of Illinois College of Pharmacy in 1978 and from the University of the Health Sciences Chicago Medical School in 1982. She completed her pediatric residency at Cook County Hospital in 1985 and her adult and pediatric fellowship in allergy/clinical immunology at Children's Memorial Hospital the following year.

Dr. Ozog holds board certifications from the American Board of Pediatrics and the American Board of Allergy & Immunology as well as other professional and scientific associations. She also serves on numerous healthcare committees and has held leadership roles in the Suburban Asthma Consortium and the American Lung Association. She is a seven-time recipient of Chicago Magazine's Chicago's Best Physicians in the specialty of allergy and immunology, as chosen by her peers over the past 21 years. Currently, in 2024 and 2025, the Chicago Magazine selected Dr. Ozog as an "Exceptional Woman in Medicine" in allergy and immunology.

Her passion for education and advocacy continues to make a lasting impact in medical and local communities. Her goal for every patient is for them to have an allergy and asthma free day.

Association Updates

2026 CCPA Annual Meeting: Time for a Check-Up – Videos Available

CCPA's Annual Meeting: Time for a Check-Up was held on Wednesday, May 13, 2026, at Fountain Blue Banquets & Conference Center. The session topics covered annual revenue cycle development, minimizing physician liability risks, and implementing artificial intelligence (AI) into pediatric practices. To view the recording of this event, please visit the Members' Portal section at www.ccpaipa.org.

CCPA Member Benefit Reminders

CCPA has added a new human resource tool called Mineral that is a compliance platform designed to streamline the administrative, regulatory and workforce-management responsibilities of organizations. CCPA members have access to Mineral's Smart Employee Handbook, which is an easy-to-use tool that helps members create and maintain a customizable and compliant employee handbook for their practices.

CCPA members have access to the American Academy of Pediatrics (AAP) Pediatric Care Online platform that contains the 33rd edition of the Red Book® and Quick Topic Review videos to provide an overview of essential point-of-care topics. This includes access to AAP's Pediatric Coding Newsletter, which also allows CCPA members to retrieve past coding issues and other pediatric coding resources, free of charge. The above AAP benefits can be accessed via the CCPA website at www.ccpaipa.org in the Members' Portal section.

Also, as a reminder, cardiopulmonary resuscitation (CPR) reimbursement is available for up to $60 for all CCPA members. Please submit your paid invoice and a copy of your CPR card to ccpa@luriechildrens.org or by fax to 312.227.9526.

CCPA Credentialing Corner

Some of the most frequent questions that CCPA staff receive are regarding CCPA's initial credentialing and recredentialing processes. Therefore, practice staff and members can find written instructions on how to complete the initial and recredentialing Illinois applications, practice checklists for both processes, and much more. Credentialing Corner can be accessed on CCPA's website at www.ccpaipa.org in the membership section.

Lurie Children's Physician Services Webpage

The Physician Services' department webpage, can be accessed at luriechildrens.org/physicianservices, it includes the following resources:

- Satellite clinic schedules
- Referral and consultation to/from Lurie Children's
- Community Provider Symposium Video Library
- LurieMD Provider Call Line (1.855.LurieMD or 1.855.587.4363)

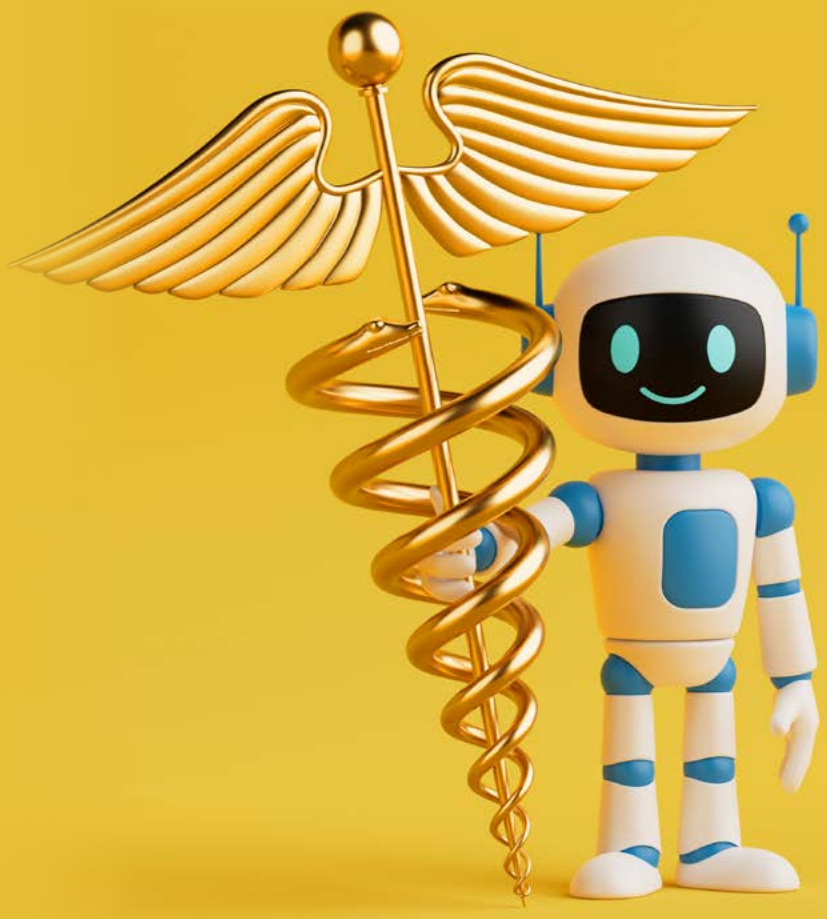
CCPA Purchasing Partners, LLC

CCPA Purchasing Partners, LLC (CCPAPP) is an industry leading group purchasing organization that leverages the collective purchasing power of multiple physician practices to negotiate better prices with suppliers. By joining CCPAPP, independent practices can access discounted rates on vaccines, medical supplies, equipment, pharmaceuticals, and other essential items, resulting in cost savings. CCPAPP is free to join with no monthly or annual dues. All eligible members receive an annual administrative award payment based on member purchases. Moreover, CCPAPP staff are knowledgeable, they provide exceptional customer service, and are committed to supporting your practice. Please call Paresh Patel, Director of Operations, to join, at 312.227.7436 or email him at papatel@ccpapp.org.

Understanding, Using, and Protecting Yourself from AI in Healthcare

A practical guide for independent pediatric practices on enabling artificial intelligence (AI) safely, the cybersecurity risks to watch, and the guardrails to put in place this quarter.

By Aaron Pritz, CEO, Reveal Risk



It is a regular Tuesday at the practice. In room one, a pediatrician dictates a visit note while an ambient scribe quietly listens, transcribes, and drafts the patient chart entry. At the front desk, a billing manager pastes a response to a denial letter into ChatGPT to "reword it more politely." An overwhelmed front desk administrator uploads next week's patients schedule into a free AI app that promises to "optimize" the flow.

Those three people might not tell you, or even realize, they are "using AI," yet all three are. And depending on which tools they picked, one of them just put protected health information (PHI) into a system with no business associate agreement (BAA), no audit trail, and no way to get the data back.

AI is already inside your practice, often running in the background of tools you already pay for. The real question is *whether you are adopting it on purpose or by accident*, and whether you have guardrails in place to protect your patients, your staff, and your license.

This article is for the independent practices in the Children's Community Physician Association who are somewhere on that spectrum: some of you are quietly experimenting with AI and may be creating risks you have not seen yet; others are holding back and missing safe productivity wins your peers are already getting. Both groups need the same thing: a clear, practical framework for moving forward with AI appropriately, without getting burned.

You probably already have AI. Therefore, you have to find it before you can govern it.

When most people picture "AI in practice," they picture ChatGPT. Frankly, that is the smallest part of the story.

AI features are now embedded in tools you already use every day: transcription utilities, coding and billing suggestions, patient messaging triage, scheduling optimization, voicemail transcription, fax-to-text, and the AI assistants built into Microsoft 365 and Google Workspace. If your electronic health records (EHR) vendor has pushed an update in the last twelve months, you almost certainly have AI features on your system. Some are turned on by default. Some can be turned on by an end user clicking a button.

Practices affiliated with a larger hospital system may have an extra wrinkle. Your hospital's EHR interface may have AI features enabled (or disabled) for reasons that have nothing to do with your practice. Affiliated group and hospital system policies may already govern what you are and are not allowed to do. Making assumptions is dangerous; even without specific details, therefore, inquire for any policy or guidance that pertains to your practice.

First, before you put any new rules in place, do a quick AI inventory. Ask your office manager and your EHR vendor four questions:

1. Which AI features are currently active in our system?
2. Which features can be enabled by an end user without administrator approval?
3. Is the BAA current, and does it explicitly cover the AI functionality?
4. And what consumer AI tools (ChatGPT, Gemini, Microsoft Copilot, Otter, etc.) are staff using on the practice's devices?

QUICK CHECK | Is It AI?

Six everyday tools that probably have AI inside, whether you turned it on or not:

- EHR ambient documentation or "scribe" features
- Coding and billing suggestion engines
- Patient messaging triage and auto-reply
- Voicemail transcription and fax-to-text
- Microsoft 365 Copilot and Google Workspace AI
- Phone systems with "smart" call routing or summaries

Two practices, two mistakes

Picture two practices in the same network or community of physician offices.

Practice A is enthusiastic. The office manager loves new tools. Staff use ChatGPT for everything: drafting patient letters, summarizing payer denials or follow-ups, even re-wording appointment reminders. Productivity is up. Morale is up. What no one has thought about is that those staff members are passing names, dates of birth, diagnoses, and insurance details into a public AI tool that retains data for

model training, has no BAA, and stores information in places that nobody at the practice can identify.

Practice B is the opposite. Leadership read one scary article about AI and put a blanket ban in place: no AI tools, no exceptions. Meanwhile, the practice across town has implemented a sanctioned ambient documentation tool, recovered six hours a week per physician, and is using that time to see more patients. The reality check: *Practice B is not avoiding risk*. They are just trading one kind of risk (data exposure) for another kind of risk (falling behind on efficiency, burnout, and recruiting).

Both practices got it wrong because they treated AI as a yes-or-no question. The right questions are: *Which AI?* For what *purpose*? With what *guardrails*? And under whose *policy*?

> The right question is not whether to use AI. Is it AI? For what purpose? With what guardrails? And under whose policy?

Five guardrails to put in place this quarter

Let us begin with an important financial disclaimer: None of these suggestions require a six-figure cybersecurity program. All of them can be implemented by a practice of any size within a single staff meeting and a few follow-up conversations.

1. **Know your hospital's rules first**. If your practice is affiliated with a larger hospital or health system, their AI policy, EHR configuration, and BAA likely already apply to you in some form. Do not guess here. Ask, in writing, for the current AI use policy and any guidance, training, or restrictions specific to community-based practices. Align your internal rules to theirs, not the other way around. If you are not affiliated with a larger network, you still need to write your own policy, because someone is going to ask… soon.

2. **Get the BAA, then re-read the old ones**. Any tool that touches protected health information needs a BAA. The BAA you signed with your EHR vendor years ago may not cover the AI features they have added since. Ask your EHR vendor and any other vendor that touches PHI for their current BAA and any AI-specific addendum. Read it. If they cannot produce one, that is your answer about whether to turn the feature on.

3. **Decide what can and cannot go into public AI**. Here is a simple way to start: consumer versions of ChatGPT, Gemini, Microsoft Copilot, Claude, and similar tools should never receive PHI, patient identifiers, payer-specific case details, or anything that could identify a child or family member. You can write this into a simple one-page rule, share it at your next staff huddle, and post it where staff can see it. "No PHI in public AI" is not the only rule you will eventually need, but it is the first one. Also, if you have not embraced AI and updated appropriate use of information technology (IT) policies, you are likely to have the risk of shadow AI use.

4. **Train your team on the new social engineering, including deepfakes**. Voice cloning can now be accomplished for less than twenty dollars in under ten minutes. The "doctor" calling to authorize a prescription refill, the "parent" calling about a sensitive record, or the "practice owner" emailing the billing manager to redirect a payment may not be who they say they are. We have seen real cases where attackers used a few seconds of public audio to impersonate executives and trick staff into wiring large sums. Train your team to verify on

CONTEXT CHECK | If You're Part of a Larger Hospital System

Three questions to ask before you turn anything on:

- What is our hospital system's current AI use policy, and does it apply to community-based practices like ours?
- Are the AI features inside our shared EHR governed by the hospital's BAA, or do we need our own?
- Is there training, guidance, or a help line we can route our staff and physicians to, instead of building our own?

If you do not get clear answers, escalate. The answer you write down is the one your auditors will read.

another channel (call them back at a known number), especially for anything financial or anything involving a record release.

5. **Pilot one AI use case well before you try five more**. The practices that get the most out of AI pick one use case, run it for ninety days, measure the results, and then expand. Ambient documentation, denial-letter drafting, and patient-message triage are common starting points. Pick the challenge that hurts most in your practice today, sanction one tool with a BAA, define what data it is allowed to see, and measure whether it actually saved time or improved quality. If it did, expand. If it didn't, you would only lose ninety days, not your entire AI program.

HIPAA is changing, and AI is part of the reason

You have probably heard that the Health Insurance Portability and Accountability Act (HIPAA) Security Rule is being updated. The proposed overhaul, expected to take effect in 2026 explicitly modernizes the rule for cloud services, third-party risk, and AI. In plain English: more documentation of what tools touch PHI, more scrutiny of your vendors, tighter expectations around incident reporting, and less tolerance for "we didn't know."

For now, the practical takeaway is this: any AI work that you do today should be documented as if the new rule were already in effect. Write down what tools you use, what data they see, what BAA covers them, and who decided to turn them on. If the rule lands the way most of us expect, then the practices that documented their decisions are going to have a much easier 2026 than the ones who did not.

What to do Monday morning

You do not need a project plan. You need five short conversations.

1. Ask your EHR vendor which AI features are active, and whether the BAA covers them.
2. Inventory the consumer AI tools that your staff are already using (ChatGPT, Gemini, Copilot, Otter, and similar).
3. Confirm your hospital affiliation's AI policy in writing and align your practice rules to it.
4. Write one rule: **no PHI in public AI**. Share it at your next staff huddle and post it where staff can see it. If you have trusted/practice sponsored AI tool(s), promote those and indicate that public AI should not be used for work purposes at all.
5. Pick one AI use case to pilot this quarter. Define success before you start.

A final word

AI in healthcare is not a future debate. It is a present-tense responsibility, and independent practices have more agency than they realize and less support than they often need. You do not need a hospital-sized cybersecurity program. You need clear questions, a short list of rules, and a willingness to ask the next layer up when the rules are not obvious.

If you read this article and felt a little behind, you are in good company. If you read it and felt a little ahead, help your peers in the next office over. The practices that do best with AI in the next two years will not be the ones with the biggest budgets. They will be the ones that paid attention early, asked the boring questions, and took notes.

Questions, or want to go deeper?

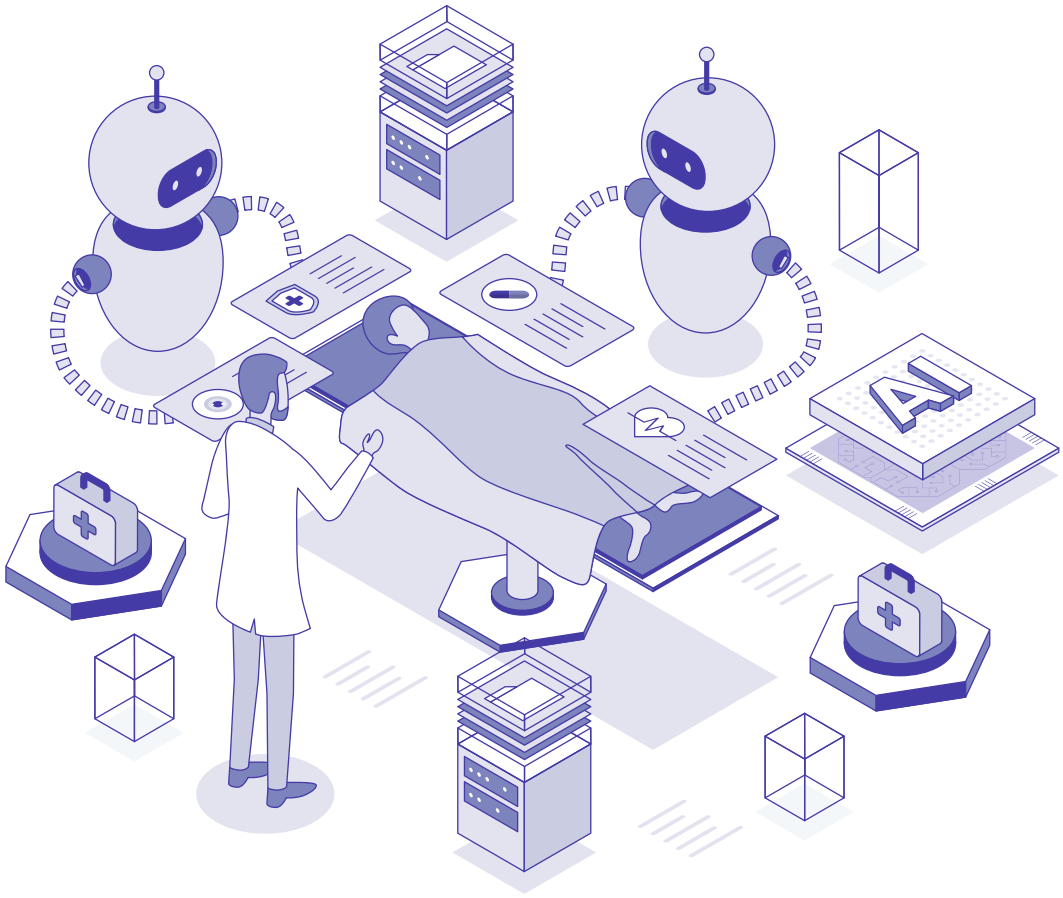
We are happy to answer questions from CCPA members at no cost.

Ask Aaron directly: aaron@revealrisk.com

Or route through the association: ccpa@luriechildrens.org

HIPAA, AI, and Your Daily Work in Chicago Healthcare

By Aaron Pritz, CEO, Reveal Risk



If it feels like healthcare cybersecurity keeps getting more complicated, you are not imagining it.

Has your practice or affiliated hospital updated its Health Insurance Portability and Accountability Act (HIPAA) to match the practice's daily workflow? Are telehealth, messaging apps and artificial intelligence (AI) tools included? For many clinicians and staff, these changes can feel like yet another obstacle between them and patient care.

There are *more* multi-factor authentication (MFA) prompts. *More* restrictions on devices. *More* questions about AI. *More* reminders not to text patient information.

However, these changes are happening for a reason.

For many healthcare organizations, HIPAA has been on autopilot for years. Organizations have been doing enough to avoid fines, but not enough to keep up with ransomware, AI-powered scams, and increasingly complex vendor relationships. Meanwhile, federal expectations are shifting, and frontline clinicians and staff will feel those changes directly in how they log in, document, communicate, and use new tools.

Modernizing HIPAA requires so much more than merely passing an audit or filling out off-hand compliance paperwork. We are talking about changing how systems are secured, how staff use them, and how patient information moves through your workflows.

This is not just an information technology (IT) problem. It is not just an administrator problem. It is about our collective priority: being able to safely care for patients without disruption.

What's Changing: Fewer Exceptions, More Non-Negotiables

In the past, some HIPAA security requirements have been treated as "optional if documented." Even when it was positioned as a last resort option to do so, essentially, if a security control did not seem reasonable, or feasible, an organization could document why they were not doing it... and move on. For example, multifactor authentication is a great security control, but often healthcare workers simply do not have the time to double-verify their identity every single time they logged into a system; documenting this bottleneck was, in the past, sufficient to justify skipping it.

That flexibility is narrowing.

Regulators are now moving to make many of those once "addressable" safeguards *mandatory*. Additionally, certain required controls, like completing a security risk assessment (SRA), which have only been enforced on an ad-hoc basis, will be mandatory, too.

In practice, this means fewer exceptions and more baseline controls that every healthcare organization is expected to have in place, regardless of size or location.

What that will likely look and feel like to you:

- **Yes, more frequent use of MFA**
  Expect more systems that require a second verification step—such as a text code, app prompt, or token—when accessing patient records or hospital applications.
- **Tighter controls on access and shared devices.**
  Shared logins, generic accounts, and workstations left unlocked will increasingly be treated as an unacceptable risk.
- **Less tolerance for "workarounds."**
  Sending protected health information (PHI) to a personal email for quick edits, texting patient details over non-approved apps, or storing data in personal cloud services (like Apple or Google) may become strictly prohibited. Some things that we do innocently, for speed and convenience, might have serious repercussions.

These changes can feel burdensome in the moment. However, they are driven by a simple reality: **attackers continue to see healthcare as a high-value, high-impact target**.

How This Affects Your Day-to-Day Work

From a clinician or staff perspective, HIPAA security updates often show up as friction points: a new login step, a blocked website, an app you cannot use anymore. Hopefully, it helps soften the blow to connect those changes back to why they are happening.

Here are some common impacts you may see:

Login and access changes

- More systems require MFA, especially for remote access or mobile apps.
- Tighter rules about who can see which patient records, even within the same service line or department.

Documentation and communication changes

- Greater emphasis on documenting within

approved systems rather than side notes, local files, or unofficial tools.
- Stricter use of secure messaging platforms instead of standard short message service (SMS), consumer chat apps, or personal email for anything involving PHI.

Device and network use

- Stricter rules on using personal devices for work (phones, tablets, laptops) unless they are enrolled and secured by the organization.
- More frequent reminders to log out, lock screens, and avoid plugging unknown USB devices into practices' computers.

While these steps add a bit of friction, they also significantly reduce the chances that one mistake, such as clicking on a phishing link, losing an unsecured device, or using an unapproved app, turns into a major incident affecting thousands of patients and forcing system downtime.

And to be clear, changing HIPAA regulations is not about security professionals not trusting healthcare professionals. We have the same goal: effective and protected patient care. While some security controls might feel cumbersome and super irritating at times, to those navigating them, ideally, we can all remember we are on the same team.

AI in the Practice: Helpful, Powerful… and Risky

In many Chicago-area practices and hospitals, AI is already part of daily practice, whether it is officially labeled that way or not.

You might be using:

- Scribe tools that listen to patient encounters and draft notes.
- AI assistants in your electronic health records (EHR) that summarize histories or suggest documentation.
- Online AI tools to help draft patient letters, education materials, or appeals.

From a HIPAA perspective, any AI tool that sees identifiable patient information is treated like any other vendor handling PHI. That means:

- Your organization must have a formal agreement (often a Business Associate Agreement or BAA) that specifies how that AI tool uses, stores, and protects patient data.
- "Trying out" new AI tools with real patient details can unintentionally expose PHI outside of secure systems.

A few practical guidelines for using AI safely in your work:

- **Use only approved AI tools for anything involving PHI.** If you are not sure a tool is approved, assume it is not. Ask before using it with live patient data.
- **Help your organization understand where AI is really being used.** If you have adopted AI-based tools in your workflow (even informally), let your privacy, security, or compliance contacts know. They can work to evaluate and, if appropriate, bring those tools into a governed, approved list.
- **Support clear boundaries and human review.** Many AI-driven suggestions or drafts can improve efficiency, but clinical judgment still matters. Make sure decisions that significantly affect diagnosis, treatment, or access to care remain under human oversight, even when AI is involved.

Used thoughtfully, AI can reduce burnout and improve documentation and communication. Used carelessly, it can create large, hard-to-detect exposures of PHI and introduce errors into patient care.

Why This Matters in Chicago

HIPAA is a federal law, so its core requirements apply equally in Chicago and everywhere else in the U.S. What's specific about Chicago is the scale and visibility of incidents.

In a dense healthcare ecosystem with large hospital systems, specialty centers, and community practices all interconnected:

- A single ransomware event or data breach can ripple across many sites and partners, disrupting care and operations.
- Significant incidents often become public quickly, with consequences for patient trust, reputation, and community relationships.

Every physician, nurse, tech, and administrative team member plays a role in preventing disruptions and protecting patient trust. Your community, your organization, your neighborhood, your city, are relying on you.

What You Can Do This Year

Great news for everyone: you do not need to be a security expert to make a meaningful difference. In fact, a few practical actions will have far more impact than any single new technology.

For physicians:

- Use only approved systems and tools for documentation, messaging, and AI assistance.
- Participate in risk assessments, training, and workflow mapping when asked—your insight into how work really happens is critical.

For nurses and clinical staff:

- Treat your login and badge as strictly personal; never share your credentials.
- Log out or lock shared workstations when you step away, even briefly.

For administrative and support staff:

- Be extremely cautious with unexpected email links, attachments, or login prompts; when in doubt, report rather than click.
- Use secure, approved channels for schedules, reports, and any lists or documents that include patient identifiers.
- If something feels off or is particularly urgent, verify the request through a separate channel that you are confident about.

For everyone:

- Speak up if something feels off, whether it is a suspicious email, a device acting strangely, or a process that pressures people into unsafe shortcuts.
- Ask questions about new tools (especially AI tools): Is this approved? How is patient data protected? Who can see what we put into it?

Modernizing HIPAA is not just about complying with new rules and the fear of compromising patient care. It is more about security professionals working with healthcare professionals. It is about making thoughtful choices, not just the fastest ones.

The future of healthcare will not be less digital. It will be more digital, more connected, and increasingly powered by AI.

The organizations that thrive will not be the ones that avoid these changes. They will be those that adopt them thoughtfully, protect patient trust, and keep patient care at the center of every decision.

About the Author

Aaron Pritz is the CEO of Reveal Risk, a boutique cybersecurity consulting firm based in Carmel, Indiana. Reveal Risk is practitioner-led and tool-agnostic, with a particular focus on helping healthcare, pharma, and other regulated organizations build practical cybersecurity, governance, and human risk management programs. Aaron and his team work with clients ranging from independent physician practices to global enterprises. He hosts the Simplifying Cyber podcast and writes The Risk Realist newsletter on LinkedIn.

Reveal Risk | 650 East Carmel Drive, Suite 340 | Carmel, IN 46032 | revealrisk.com