

CEP

MAGAZINE

A PUBLICATION OF THE SOCIETY OF
CORPORATE COMPLIANCE AND ETHICS

DANIELLE HERRICK

VICE PRESIDENT OF RISK, COMPLIANCE
AND ETHICS AT BLOOM ENERGY

KEEPING IT REAL (P10)

Building an AI-powered
workflow for ethics and
compliance: A seven-step
model (P16)

Keep suspension and
debarment from knocking
on your door (P24)

The whistleblower is not
the risk; mishandling the
report is (P30)

Strategic board engagement
through compliance
intelligence: How to be heard
and create action (P36)





AI IS ALREADY AFFECTING YOUR PRIVACY PROGRAM: ARE YOU PAYING ATTENTION?

by Micki Jernigan



Micki Jernigan
JD, MPH, CHC, CHPC, CCEP
(micki.jernigan@genzeon.com)
is the Senior Vice President of Privacy and Compliance and Chief Privacy Officer at Genzeon in Exton, Pennsylvania, USA.

Artificial intelligence (AI) is no longer a futuristic concept. In fact, it's already embedded in daily operations throughout the healthcare industry. Whether it's reviewing messages in patient portals, flagging readmission risks, or parsing free text for clinical coding, AI tools are already at work. Often, they operate quietly, with little fanfare and even less oversight.

For privacy professionals, this is both a challenge and a call to action. The question isn't whether AI has affected your organization's privacy program; it's where and how deeply. And if you haven't audited or evaluated your AI exposure yet, now is the time.

A phrase we often like to use is, "Privacy officers aren't the office of 'No.' We're the office of 'Know.'" One of the secrets to successful AI usage is keeping your privacy officer informed, preferably prior to implementation.

The two faces of AI:

Generative versus non-generative AI in healthcare comes in two major forms: non-generative and generative.

Non-generative AI supports decision-making based on existing data. Common uses include:

- ◆ Classifying emails as spam
- ◆ Predicting housing prices or patient readmissions
- ◆ Recommending streaming content or clinical next steps
- ◆ Detecting insurance or billing fraud
- ◆ Assisting coders via natural language processing (NLP)

This form of AI has been integrated into systems like electronic medical records (EMRs), revenue cycle tools, and risk modeling platforms for years — often without being explicitly labeled as "AI."

Generative AI, on the other hand, creates new content — letters,

clinical summaries, policy drafts. Popular examples include tools like ChatGPT or Microsoft Copilot. These tools raise entirely new questions around data use, transparency, and regulatory exposure, especially when the AI is trained on sensitive or confidential patient, employee, or business data.

Understanding the difference is essential for compliance professionals. Non-generative AI is often preapproved or embedded in tools. Generative AI — especially third-party or public-facing models — presents emerging risks that require deliberate oversight.

It's already in use, but is it under control?

AI use is expanding — sometimes without formal compliance input. Consider the following areas where AI might already be embedded within your organization:

- ◆ **EMRs:** AI triages messages, suggests medication refills, or flags sepsis risks.
- ◆ **Coding:** NLP tools extract billing codes from free-text documentation.
- ◆ **Security:** Facial recognition scans for weapons or suspicious activity.
- ◆ **Human resources:** AI may assist with resume screening or training analysis.
- ◆ **Policy review:** Software compares institutional policies to new regulations.
- ◆ **Visitor management:** Unmanned kiosks may scan IDs and print badges automatically.

In each of these examples, AI is being used to improve efficiency. But every use case that touches patient information, employment data, other personally identifiable information (PII), or internal communications requires

compliance oversight. If these tools have been implemented without your privacy officer's input, now's the time to ask tough questions.

The privacy officer's expanding role

Privacy professionals must adapt to the AI age — not just as risk mitigators, but as strategic advisers. The compliance and privacy functions must evolve from reactive to proactive. This includes:

- ◆ Educating stakeholders across the organization
- ◆ Reviewing vendor contracts and business associate agreements for AI-specific clauses
- ◆ Creating clear approval processes for new AI tools
- ◆ Monitoring tool usage for protected health information (PHI), PII exposure, or policy violations
- ◆ Auditing for fairness, bias, and appropriateness of AI-generated outputs

The privacy officer's scope must expand beyond traditional PHI protection to include business data, financial information, and employee records — any of which may be processed by AI engines.

Building privacy guardrails before it's too late

With federal legislation on AI still limited in the U.S., healthcare organizations must carefully navigate the growing patchwork of state legislation and create their own safeguards. These are three potential governance models:

1. **Strict prohibition:** Some organizations, upon discovering unapproved AI tools, have halted all AI use until policies and oversight are in place.

2. **Committee-based review:** More balanced, this model requires privacy, legal, IT, and operational leaders to jointly review all AI use cases before implementation.
3. **Tiered permissions:** The most flexible model, it allows certain low-risk uses (e.g., internal tools without PHI) while requiring oversight for more complex or sensitive applications.

Privacy professionals must adapt to the AI age — not just as risk mitigators, but as strategic advisers. The compliance and privacy functions must evolve from reactive to proactive.

Regardless of the model, privacy professionals should ensure policies address:

- ◆ Submission processes and review timelines
- ◆ Escalation paths for high-risk tools
- ◆ Penalties for bypassing oversight
- ◆ Clear exceptions policies, approved only at the executive level
- ◆ Regular audits and periodic re-reviews of approved tools
- ◆ Guardrails are not designed to inhibit innovation; they create safe zones in which innovation can flourish without regulatory missteps



**The ethics of AI:
A compliance concern**

Legal compliance is one layer of the challenge — ethical use of AI is another.

AI models can reflect and even amplify bias if trained on limited or non-representative data. A clinical model may overlook how a disease presents differently based on race, age, or sex. A billing tool might flag outliers based on flawed assumptions.

Transparency is also key. When AI influences a decision — be it a denied claim,


a clinical recommendation, or an auto-generated letter — patients and staff deserve to understand how that decision was made.

And then there's data privacy. Uploading internal documents or PHI into tools like ChatGPT or Copilot can violate HIPAA and erode organizational trust. Doing so would be like "posting the data on a billboard."

That's why employee training is vital — particularly for students, residents, and early-career clinicians who may not realize that generative AI tools are public, not private.

Final thoughts: The privacy office as a strategic enabler

AI isn't the future; it's now. And while the tools may be fast-moving, your privacy program doesn't need to play catch-up.

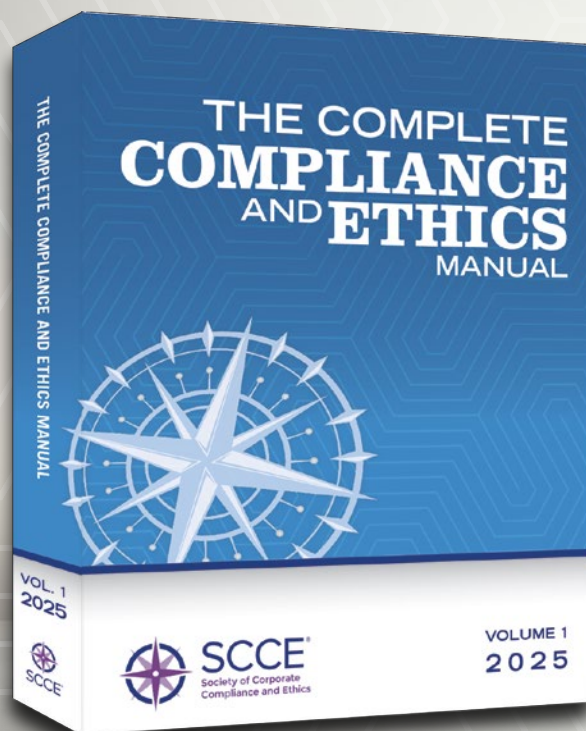
Privacy professionals are uniquely equipped to guide AI adoption that is ethical, lawful, and aligned with patient and organizational trust. By taking the lead, privacy officers can ensure AI strengthens healthcare — not at the cost of its integrity, but in service of it. 

Takeaways

- ◆ Audit your current artificial intelligence (AI) exposure. Your organization may be using more AI than anyone realizes. Start with a discovery process across departments.
- ◆ Establish a governance framework. Define what kinds of AI require review, who reviews them, and how decisions are tracked.
- ◆ Educate staff at all levels. Ensure that everyone — from coders to clinicians to learners to executives — understands AI's boundaries and risks.
- ◆ Create a protocol with enforcement. Policy is meaningless without defined consequences. Noncompliance must carry weight.
- ◆ Don't wait for legislation — lead now. Regulation is coming, but compliance leaders don't need to wait. Start building a culture of responsible AI use today.

The go-to resource every compliance library needs – updated for 2025!

The Complete Compliance and Ethics Manual 2025 is now available! This updated resource will help you keep your compliance program moving forward with new and updated analysis, information, and tools based on the most current industry developments.



What's new for 2025?

- **11 new articles including:**
 - Managing the Ethics and Compliance Risks of Artificial Intelligence
 - Methods and Guidelines for Demonstrating Compliance Program Effectiveness
 - How to Protect Compliance Risk Assessments from Unwanted Disclosure
 - Focusing on Trust: How to Elevate Board Oversight to Advance Compliance and Ethics Culture
 - Navigating U.S. Privacy Standards: A Guide for Compliance Officers
- **Updated articles and appendices**

Available in three purchasing options



One-year
online subscription



Two-volume softcover
book set



Money-saving
print + online bundle

Learn more and purchase
corporatecompliance.org/CCEM

