COSMOS
Navigate the Compliance Universe

Compliance Today - May 2024

**Karen Habercoss** (karen.habercoss@uchicagomedicine.org, linkedin.com/in/karenhabercoss/) is the Chief Privacy Officer at the University of Chicago Medicine & Biological Sciences in Chicago, IL.

**Emmelyn Kim** (ekim@northwell.edu, linkedin.com/in/emmelynkim/) is the Vice President, Research Compliance & Privacy Officer at The Feinstein Institutes for Medical Research, Northwell Health in Manhasset, NY.

# Hey AI, tell me about privacy in healthcare and research

by Karen Habercoss, MBA, MSW, CHC, CHPC, CHRC, CCEP, CDPSE, CIPM, and Emmelyn Kim, MA, MPH, MJ, CHRC

General use of artificial intelligence (AI) became available through OpenAI's introduction of ChatGPT—a chatbot—on November 30, 2022. This led to broader public adoption of the technology, quickly reaching 100 million users in two months.[1] However, the quick uptake and pace of AI development had led to concerns and calls for global generative AI regulation by the CEO of ChatGPT in 2023 during congressional testimony.[2]

Additionally, over 1,000 technology leaders and researchers called for a pause to advanced AI development, citing risks.[3] Despite AI's rapid development and use, risks may still be unknown; therefore, guardrails through regulatory frameworks may be required.

The EU has already been leading efforts to develop the world's first comprehensive AI regulatory framework through its AI Act as part of its digital strategy. This framework was proposed by the European Commission in April of 2021 and is centered on the development and use of AI classified by risk to the health and safety or fundamental rights of a person.[4] The EU AI Act—recently passed by the European Parliament in March 2024—is anticipated to be in force by mid-2026.[5]

The U.S. government has also taken some preliminary steps to address AI by publishing a draft blueprint for an AI Bill of Rights outlining five principles and associated practices to promote trustworthy AI. This includes privacy standards and rigorous testing before AI becomes publicly available.[6] President Joe Biden also issued an Executive order on Safe, Secure, and Trustworthy Artificial Intelligence on October 20, 2023.[7] The directive serves to promote new safety and security standards while protecting privacy and advancing equity and civil rights, among other aims. As calls for regulation grow, the EU and U.S. announced a collaborative effort to develop a voluntary AI code of conduct to harmonize practices, set standards and principles for AI development and governance while regulations are developed and work their way through legislative processes.[8]

In the U.S. healthcare industry, the use of generative AI presents not only many opportunities but also risks if not carefully vetted, implemented, and monitored. One of the major risks of using AI in the healthcare industry that compliance and privacy professionals and businesses must pay attention to is the potential for privacy violations of regulated data. Additional concerns include security, protection of intellectual property and proprietary information, and ethical concerns.[9] As compliance and privacy leaders in healthcare and academic research

settings assess risks, policy gaps, and develop future work plans, the following are some potential considerations for AI.

## AI overview

Loosely defined as computer software or machines that can represent human intellect independently, AI in healthcare may take several forms. Common types include machine learning (ML), deep learning (DL), generative AI, and large language models (LLM). Overall, what is important to recognize is that AI requires large amounts of information and data to train its models for accuracy and validity. As the name implies, machine learning involves using computers to adapt and make conclusions after being trained with sequenced operational instructions—also called algorithms—and large data sets. Deep learning builds from machine learning to further recognize and demonstrate multifaceted patterns within data that humans otherwise wouldn't easily identify. Generative AI uses algorithms and data inputs to produce novel data, images, video, text, code, or other content types for further use. LLMs are specifically focused on creating text and linguistics similar to a human's use of language.

Some examples of current clinical uses of AI in healthcare are chatbots interacting with patients to assist in appointment scheduling or the processing of prescription refill requests, the transcription of the physician–patient verbal interaction during a visit into medical record documentation and coding, analysis of radiologic scans as an augmented review to propose medical interventions, remote patient monitoring of sleep patterns or blood pressure through a wearable or implantable device, smaller development cycles for new medications undergoing research, development, and trials, and greater user accuracy in robotic surgery.[10] Healthcare payers can use AI to synthesize claims management data or identify potential for fraud. All of these and more hold great promise for the future of healthcare for efficient and quality-based patient care as long as privacy issues are considered. The use of patient and healthcare consumer information in AI technologies can present problems in the areas of consent for data collection, data retention, transparency and secondary use of data, limitations and minimum necessary requirements, and unintended consequences of data spillover where information is obtained for unplanned individuals.[11] These—in addition to potential for re-identification and data inadvertently or impermissibly shared with external third parties—can have trust, regulatory, and legal consequences, with conviction in the use of AI being one of the strongest concerns. According to a Pew Research Center report, 60% of Americans express discomfort with the use of AI for disease management.[12]

Even as formal regulations are being deliberated and enacted and the landscape is ever-evolving, there should be a continuous and conscious effort to evaluate the use of AI against all relevant current federal, state, and international laws, with HIPAA and the EU General Data Protection Regulation (GDPR) being primary ones. Both contain principles that already address privacy requirements that will need to be appraised concerning AI. Maintenance and enhancement of current policies and procedures remain applicable as with any new or emerging area of technological influence. AI, at its core, is technology-driven and, therefore, should follow a similar privacy analysis, risk review, and mitigation planning cycle that would be performed when any new process or technology that uses data is introduced into a healthcare environment. In this case, it involves significantly larger scopes of service, scaled sizes, and amounts of data inputs, thereby potentially increasing the privacy risk.