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.

Healthcare considerations

One initial consideration is whether current policies and procedures sufficiently account for an AI model developed internally, with its own data for the sole use of the entity, or the AI is purchased through a third-party vendor, whether the AI is publicly available for use. Each scenario requires its own deliberation and needs updated governance. Generally, an entity that develops its own algorithms and trains proprietary AI with its own data

may seek to do so for its own internal quality or research initiatives. It may want to consider how much and what types of data can be used following HIPAA and regulatory requirements such as minimum necessary standards or contemplate the transparency of its data use to patients and consumers through its privacy notices and the maintenance of confidentiality with the security of its systems with technology and IT security.

AI purchased for healthcare uses through a third-party vendor often requires valid contractual agreements that define the data specifications up-front and offer legal and regulatory protections if a data breach occurs by a third party—especially with the data size. The business' standard supply chain, technology feasibility, and procurement processes should consider AI and privacy requirements in addition to privacy by design. It can be helpful for compliance and privacy departments to be stakeholders as part of these processes by providing guidance on privacy requirements and best practices.

Considerations under HIPAA for third-party AI technologies accessing protected health information (PHI) include using valid business associate agreements. Other international laws may also require certain contracts to be in place, depending on the relationship. The business owner of the data must be aware of and consider further use of data by the third party. This could be in de-identified form to continuously train the third party's AI models either for the benefit of the software program that the entity is a party to for enhancements or even for use in the third party's development of their own future products that the business may not choose to purchase. The business needs visibility and knowledge into potential secondary data uses regardless of the data form. This includes whether the third party indicates that data will be de-identified and aggregated with other nonaffiliate companies' data as a condition of purchasing the product or service. This could present a risk of little to no ability for the business to verify if the data is actually de-identified or anonymized in compliance with regulatory requirements. Also, the business needs to consider the level of cybersecurity incident and liability coverage the third party offers. Both issues may impact the business decision about purchasing and using third-party AI software—even if the use case could offer potential benefits in patient clinical care.

The use of free, publicly available, generative AI in healthcare poses regulatory and legal risks. Data added to public AI technology, such as ChatGPT, could be used to continuously train public models. As a result, it may increase the risk of impermissible acquisition, access, use, or disclosure of data under HIPAA and other federal, state, and international privacy laws if shared with the company and other users without the required contracts and protections. Other risks may be unknown due to lack of visibility into how publicly available AI technologies accumulate, use, and share the inputs.[13] Therefore, evaluate strategies for education and training to the business on the hazards of entering and storing sensitive, confidential, or regulated data such as personally identifiable information, PHI, highly confidential information, or even nonregulated company strategic data.

Once the compliance and privacy departments obtain an understanding of the business vision and strategy for AI use and a review of laws and relevant regulatory responsibilities occurs, a gap analysis could be conducted. This can assist compliance and privacy in working with key business stakeholders throughout the organization to ensure privacy requirements are understood in each area. This can include IT, marketing, clinical operations, health information management, finance and revenue cycle, research, and other vital areas.

Because the dependability of AI systems in healthcare is reliant upon large volumes of medical data, including those of special populations such as children or that of highly sensitive types—for instance, mental health, substance use, genetics, communicable diseases, child abuse, sexual assault, etc.—consider the implementation of privacy by design principles or a proposed transparency model to ensure regulatory, social responsibility, and data lifecycle items are rigorously addressed.[14] Emerging and current privacy enhancing technologies and techniques like differential privacy, use of synthetic data, encryption, distributed analytics, role-based access procedures, can have both respectable applications and challenges with AI that compliance and privacy

professionals should be aware of.[15] Figure 1 provides a brief overview.

Figure 1: Organization for Economic Co-operation and Development overview of privacy enhancing technologies with applications and challenges[16]

Types of PETs	Key technologies	Current and potential applications*	Challenges and limitations
Data obfuscation tools	Anonymisation / Pseudonymisation	Secure storage	- Ensuring that information does not leak (risk of re-identification) - Amplified bias in particular for synthetic data - Insufficient skills and competences
	Synthetic data	Privacy-preserving machine learning	
	Differential privacy	Expanding research opportunities	
	Zero-knowledge proofs	Verifying information without requiring disclosure (e.g. age verification)	- Applications are still in their early stages
Encrypted data processing tools	Homomorphic encryption Multi-party computation (including orivate set intersection)	Computing on encrypted data within the same organisation Computing on private data that is too sensitive to disclose Contact tracing / discovery	- Data cleaning challenges - Ensuring that information does not leak - Higher computation costs
	Trusted execution environments	Computing using models that need to remain private	- Higher computation costs - Digital security challenges
Federated and distributed analytics	Federated learning Distributed analytics	Privacy-preserving machine learning	- Reliable connectivity needed - Information on data models need to be made available to data processor
Data accountability tools	Accountable systems	Setting and enforcing rules regarding when data can be accessed Immutable tracking of data access by data controllers	- Narrow use cases and lack stand-alone applications - Configuration complexity - Privacy and data protection compliance risks where distributed ledger technologies are used - Digital security challenges - Not considered as PETs in the strict sense
	Threshold secret sharing		
	Personal data stores / Personal Information Management Systems	Providing data subjects control over their own data	

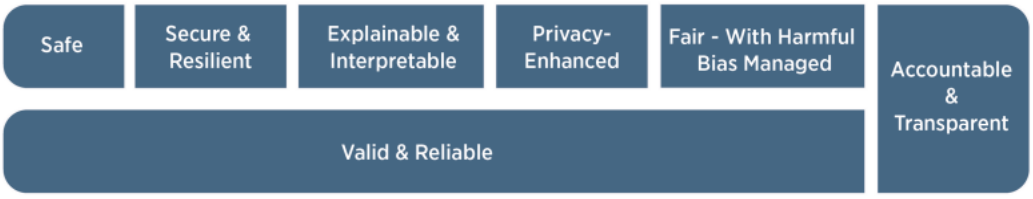
Note: (*) Only one application has been included for the sake of readability.

Compliance and privacy will want to review policies, procedures, other established internal governance structures, privacy committees, and education programs to account for AI usage. For example, productivity tools such as a free, AI-based meeting assistant that connects to business emails and calendars might consume and use available PHI and other regulated data in business meetings. Lacking a fully contracted, enterprise-compliant version of the AI meeting assistant software could potentially implicate an impermissible PHI disclosure requiring mitigation and a risk of compromise assessment for potential breach impact. Accordingly, education programs can integrate how the company uses AI while promptly reinforcing expectations from established policies and reporting concerns.

Understanding and using recognized privacy and AI frameworks helps mature an entity's overall compliance and privacy programs. It can allow for characterizing success capabilities and regulatory requirements while mapping each back to a specifically aligned business purpose.[17] Some examples include the National Institute of Standards and Technology (NIST) Privacy or AI risk management frameworks, both available on the NIST website. Establishing an AI data steering committee or incorporation into a subcommittee of a current data or privacy committee can be a way to leverage critical parts of a framework. Compliance and privacy departments will need to collaborate with leadership and employees of the business to make sure any content disseminated

from the use of AI is accurately generalizable, meets the business' own developed standard for interpretability, fairness, and lack of bias, is complete and maintains a high level of ethical standard. Figure 2 notes the NIST characteristics of trustworthy AI.[18] The use of AI technology should also align with a company's code of conduct to ensure that data use remains consistent with the organization's privacy requirements and awareness of any auditing and monitoring of AI that will happen.

Figure 2: Characteristics of a trustworthy AI systems. NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) [19]



Academic considerations

The use of AI tools in academia will also necessitate education and the development of standards and policies around their use. The International Committee of Medical Journal Editors added a section on AI-assisted technology outlining paper submission standards for authors on disclosure and appropriate use of AI.[20] This includes disclosing how AI is used in work and not allowing chatbots to be listed as authors. Ensuring human oversight of outputs is essential, especially reviewing for completeness, accuracy, and bias. Authors must also assert no plagiarism in both text and visual outputs. Researchers using publicly available AI tools to analyze study results must be careful about uploading PHI and other proprietary and sensitive information without the appropriate agreements and safeguards in place. Given the public's use of AI tools, consider incorporating this topic in academic and ethical and responsible conduct of research curriculums to modernize education at academic and research institutions. Discussions on ethical use, privacy, security, and integrity are essential elements to include. Compliance and research integrity officers may need to anticipate such issues and think about technical and subject matter expert approaches to handle research misconduct allegations involving AI.

In-house research and development of AI/ML tools

Internal research and development of AI/ML technologies in the academic healthcare setting requires additional considerations. This includes the appropriate infrastructure and governance to vet and evaluate the process, including development, use, and monitoring for performance and risks. The development of software that uses AI algorithms may not be considered human subjects research per the federal regulatory definition early on—especially if being developed and tested using de-identified data. As a result, this may preclude review by an institutional review board (IRB) but may necessitate review by an ethics committee with the expertise to review AI/ML. Even when the project requires IRB review, ensuring that the appropriate ethical questions tailored to AI/ML projects are asked and having committee members with the expertise to review such projects will be necessary. This may require established IRBs to develop separate applications and workflows for AI/ML projects.

Human subjects research regulations have yet to be modernized and may present challenges in their interpretation with AI/ML technologies. The Secretary's Advisory Committee on Human Research Protections (SACHRP) published IRB Considerations on the Use of Artificial Intelligence in Human Subjects Research to address such challenges.[21] This includes reevaluating the definition of human subject research and the use of identifiable private information in the context of AI, which one could argue that an individual could be identified

in a de-identified data set with enough data. They also acknowledge that such AI/ML projects will likely require a waiver of informed consent (and a HIPAA authorization waiver) due to the size of data sets involved in conducting the research practicably; thus, regulatory protections could be limited. Therefore, reviewing patient privacy notices for research uses and consultation by AI governance and privacy and security committees should be considered to evaluate the privacy and ethical risks and mitigation factors.

Regulatory knowledge of the U.S. Food and Drug Administration (FDA) rules is essential, especially as some AI/ML-based software are considered medical devices as per section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). Technologies classified by the FDA as Software as a Medical Device require regulatory oversight. Recognizing the acceleration in this area, the FDA published its regulatory approach and proposed framework for AI/ML technologies.[22] The FDA also released guidance on Clinical Decision Support software with criteria and specific examples of when such software would be considered a medical device as per the FD&C Act.[23] Furthermore, the FDA released final guidance on cybersecurity for medical devices that will need to be considered.[24] Therefore, having regulatory and IT expertise to review and weigh in on regulatory and security considerations for AI/ML software development will be imperative for review of in-house developed AI/ML projects and research protocols.

Often, AI may be developed in partnership with an external third party or entity seeking to commercialize products. It will be necessary to ensure that appropriate agreements are in place regarding the use of the data, licensing, intellectual property, and privacy and security safeguards. Lastly, thinking about the long-term plan around cost, maintenance, troubleshooting AI/ML software, evaluation of performance, and monitoring over time is vital, especially if being used for healthcare and quality purposes.

Conclusion

Compliance and privacy professionals can stay ahead by upskilling and learning about how their entity currently uses AI and its future strategy and use cases. Tracking regulatory developments domestically and globally will be crucial, as this will require organizations to update their infrastructures, policies, educational programs, and contracting processes. This includes evaluating structures to enable effective review and oversight of AI for clinical, operational, and research use.

Compliance and privacy leaders should consider including AI in developing their privacy programs through a recognized framework, risk assessments, monitoring, and discussions with the board and executive leadership. Most importantly, compliance and privacy professionals need a seat at the table to gain first-hand knowledge of how their own business is currently and contemplating future use of AI. Ideally, stakeholders and cross-functional committees are consulted by the business before establishing an AI strategy, initiating and maintaining corresponding governance, and throughout the progress of internally developed AI models. Finally, developing and maintaining policies and guidance that evolve with emerging technologies and new risks will be paramount.

Takeaways

- Reviewing current and future artificial intelligence (AI) business use cases requires up-to-date knowledge of the evolving privacy regulatory landscape.
- Publicly available, nonenterprise versions of generative AI pose privacy risks due to the potential for impermissible disclosures under the law.
- Using a recognized privacy and AI framework can help measure the successful adherence of business use

cases to requirements.

- The use of AI tools academically requires the development of standards, policies, and education on ethical and responsible use.
- In-house AI/machine learning development and research requires appropriate governance, review, regulatory knowledge, and monitoring.

1 Krystal Hu, "ChatGPT sets record for fastest-growing user base - analyst note," *Reuters*, February 2, 2023, https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/.
2 Mark Milian, "AI News This Week: US Congress, G-7 Caution and ChatGPT at School," *Bloomberg*, May 20, 2023, https://www.bloomberg.com/news/newsletters/2023-05-20/chatgpt-founder-and-openai-ceo-sam-altman-calls-for-ai-regulation-the-latest.
3 Future of Life Institute, "An Open Letter: Pause Giant AI Experiments," March 22, 2023, https://futureoflife.org/open-letter/pause-giant-ai-experiments/.
4 European Parliament, "EU AI Act: first regulation on artificial intelligence," updated June 14, 2023, https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
5 Patrick Austin, Ross Broudy, and Elizabeth Burgin Waller, "EU AI Act will be world's first comprehensive AI Law," Woods Rogers Vandeventer Black, March 14, 2024, https://www.jdsupra.com/legalnews/eu-ai-act-will-be-world-s-first-3716166/.
6 The White House, Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights, Making Automated Systems Work for the American People," October 22, 2022, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
7 The White House, "Fact Sheet: President Biden Issues Executive Order on Safe, Secure and Trustworthy Artificial Intelligence," October 30, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.
8 Associated Press, "Artificial Intelligence: Voluntary Code of Conduct and Regulation," May 31, 2023, https://apnews.com/article/artificial-intelligence-voluntary-code-of-conduct-regulation-585f2aaff6bfbdbcee572b347fa97cff.
9 G.P. Kanter and E.A. Packel, "Health Care Privacy Risks of AI Chatbots," JAMA 330, no. 4 (2023): 311–312, https://doi.org/10.1001/jama.2023.9618.
10 Erin Laviola, "What Types of AI Are Being Used in Healthcare?" *HealthTech Magazine*, July 11, 2023, https://healthtechmagazine.net/article/2023/07/types-ai-in-healthcare-perfcon.
11 Guy Pearce, "Beware the Privacy Violations in Artificial Intelligence Applications" *ISACA*, May 28, 2021, updated January 30, 2023, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/beware-the-privacy-violations-in-artificial-intelligence-applications.
12 Alec Tyson et al., "60% of Americans Would Be Uncomfortable With Provider Relying on AI in Their Own Health Care," *Pew Research Center*, February 22, 2023, https://www.pewresearch.org/science/2023/02/22/60-of-americans-would-be-uncomfortable-with-provider-relying-on-ai-in-their-own-health-care/.
13 Anurag Lal, "Generative AI: Its value and risks for physicians," *Medical Economics*, December 14, 2023, https://www.medicaleconomics.com/view/generative-ai-its-value-and-risks-for-physicians.
14 Shlomit Yanisky-Ravid and Sean K. Hallisey, "'Equality and Privacy by Design': A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes," *Fordham Urban Law Journal* 46, no. 2 (2019): 428–486, https://ir.lawnet.fordham.edu/ulj/vol46/iss2/5.

15 OECD, *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches*, OECD Digital Economy Papers, No. 351, March 2023, https://www.oecd-ilibrary.org/deliver/bf121be4-en.pdf?itemId=%2Fcontent%2Fpaper%2Fbf121be4-en&mimeType=pdf.
16 OECD, *Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches.*
17 Ramesh Ramani, "Generative AI Frameworks For Practical Business Implementation," *Forbes*, August 28, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/08/28/generative-ai-frameworks-for-practical-business-implementation/?sh=574b9bd1709f.
18 National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," January 2023, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
19 National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)."
20 International Committee of Medical Journal Editors, "Defining the Role of Authors and Contributors," Recommendations for the Conduct, Reporting, Editing, and Publication of Scholarly Work in Medical Journals, https://www.icmje.org/recommendations/browse/roles-and-responsibilities/defining-the-role-of-authors-and-contributors.html.
21 U.S. Department of Health and Human Services, "IRB Considerations on the Use of Artificial Intelligence in Human Subjects Research," SACHRP Recommendations, approved October 19, 2022, https://www.hhs.gov/ohrp/sachrp-committee/recommendations/irb-considerations-use-artificial-intelligence-human-subjects-research/index.html.
22 U.S. Food and Drug Administration, "Artificial Intelligence and Machine Learning in Software as a Medical Device," January 22, 2021, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.
23 U.S. Food and Drug Administration, "Clinical Decision Support Software: Guidance for Industry and Food and Drug Administration Staff," September 2022, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software.
24 U.S. Food and Drug Administration, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions: Guidance for Industry and Food and Drug Administration Staff," September 2023, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions.