Privacy, Security and AI in the Workplace

12/1/2025

Recent polls and news articles indicate that a significant portion of the workforce is using artificial intelligence (AI) tools for work purposes. Absent organizational regulation, training and oversight, employees will use these tools as they see fit. This puts healthcare organizations at risk of breach of both protected health information and confidential business information, among other risks. Many AI tools use "generative" AI, a type of artificial intelligence designed to produce new material—such as text, images, audio, and other output—based on patterns the model has "learned" from large collections of data. The model is continuously hungry for more and more data, that is, "input." Because generative AI models are typically built on large, shared model architecture, data provided in the form of "prompts" may be stored somewhere the organization does not control, may be processed along data provided by outsiders, is often used to "train" and "improve" the model, may be handled by multiple vendors and subprocessors, and may be retained in unexpected or unknown ways. Resultingly, a healthcare organization's data may be at significant risk when workforce members use generative AI tools, especially without governance and oversight.

This is true even when the user believes inputted data has been de-identified. Generative AI models can piece together rare combinations of facts, distinctive data, narrative patterns, biographical details and other input, which could result in the model being able to attach specific health and other personal information to a specific individual. Healthcare organizations can address these and other risks through a combination of:

- Governance—establishing and deputizing a cross-functional AI governance committee responsible to oversee AI management and workforce training
- Vendor/App Vetting—adopting protocols for vetting potential AI apps and scrutinizing AI vendor contracts
- Regulatory Compliance Initiatives—establishing and implementing legal and regulatory compliance initiatives

• Ongoing Monitoring—monitoring workforce activity, obtaining workforce feedback, conducting periodic compliance audits, and staying abreast of changes in law and in the AI marketplace.

Click Here to read the entire December 2025 Healthcare Law Update now!

If you would like a copy of our Compliance Checklist for Effective Management of AI in the Workplace or assistance with your organization's privacy and security program, please contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com

Authors

The following attorneys contributed to this insight.

Lani M. Dornfeld

CHPC, Member
Healthcare Law

973.403.3136 · 973.618.5536 Fax

ldornfeld@bracheichler.com