COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 33, Number 15. April 22, 2024
Consider HIPAA Implications When Using PHI to Train AI Models, Experts Say

By Jane Anderson

Health care entities and technology companies seeking to use health data within artificial intelligence (AI) systems need a good grasp of the HIPAA implications to avoid inadvertently creating privacy risks, experts say.

Ty Kayam, principal corporate counsel for digital health, artificial intelligence, and technology transactions at Microsoft, and Jodi Daniel, an attorney with Crowell & Moring, spoke on the use of protected health information (PHI) in AI systems at the 41st National HIPAA Summit Feb. 27.[1]

"In the space of using data for AI purposes, from where I sit or what I do day to day, I really ask myself four big questions," Kayam said. "What are you trying to accomplish? What sort of universe or technology are you in? What is the use case that you want to accomplish? And when do you need data, and then what do you need?"

To answer these questions, it's essential to determine whether the data needs to be identified or can be de-identified and whether there are mechanisms that can mitigate privacy risks, she said. Any entity looking to use data for AI needs to know what laws apply on the state, federal and global levels, and consider deploying some effective AI privacy risk mitigation strategies, Kayam said.

Not all PHI is Necessary for AI

Two major types of AI models are used in health care: predictive models and generative AI, Kayam said. Predictive AI uses machine learning algorithms to learn from existing data and makes predictions or recommendations based on patterns and trends, she explained. "For example, a predictive AI model could be trained on a data set of patient health records and then used to predict if certain patients are more likely to have a specific health issue."

Generative AI uses deep learning algorithms to create new content, including text, images and code, based on existing data and user input. "A classic example would be using a generative AI model to design a potential new cancer drug based on chemical and biological data that it's been trained on," Kayam said.

In the "universe" of generative AI, there are two important models. Foundation models are machine learning models trained on a broad set of data. Large language models are a subset of foundation models that are designed specifically for language-related tasks, Kayam said, noting that ChatGPT uses large language model AI.

Data is necessary to develop and deploy AI. Specifically, data is needed for training, tuning, testing, use and deployment and for "prompt engineering," which is teaching a large language model how best to respond to specific prompts (e.g., "do not provide diagnosis" or "only provide information from the database"), Kayam said.

"So, for example, to train, tune, and test an AI model to diagnose an illness based on an X-ray, it needs lots of images of patients both with and without the illness, along with annotations and labels and metadata to explain

what it is that the model is looking at," she said. "And similarly, to use or deploy an AI model that can recommend a treatment plan, it needs the patient's current and past health information like symptoms, medication, allergies and test results."

Not all health data or PHI is necessary for AI, since some AI applications can use anonymized, aggregated synthetic data or no health data at all, Kayam said. "When you are assessing demand for hospital beds, you don't necessarily need personal details or any information about patients—you can just look at the number of beds, the number of admissions and discharges, and make predictions based on that. Whether PHI or health data is needed depends on the specific use case, the data source, and the applicable data laws that are required."