COSMOS
Navigate the Compliance Universe

# Report on Patient Privacy Volume 19, Number 9. September 10, 2019 Health Care's Adoption of AI May Bring Privacy, Security Risks

By Brett Goncher

As the technologies underpinning artificial intelligence (AI) applications advance, the tremendous potential to use analysis of patient data to increase the efficacy of covered entities (CEs) and business associates (BAs) brings privacy and security considerations under HIPAA, experts warn.

There is a lot of media hype surrounding the time- and cost-saving benefits of AI and machine learning, ranging from the automation of routine tasks to cars that drive themselves. And the first step in understanding what regulations may apply to AI technology is to agree on what AI means. That is easier said than done.

According to William Tanenbaum, shareholder at the law firm Polsinelli PC, AI in the health care more aptly refers to "augmented intelligence," which can be relied upon to assist doctors, rather than replace their decision-making. In order to properly use the conclusions that AI applications produce, there must be transparency in the factors used in complex algorithms, he explained in a recent webinar hosted by Polsinelli. Thus, in addition to the data itself, doctors will be vital to training the algorithms.

## AI is Already Here

David Holtzman, executive advisor at information security consulting and assessment firm CynergisTek Inc., sees AI as a system that learns, thinks, or acts beyond the rules or parameters of a particular programmer or controller who may or may not set the parameters of the data. "Think of it as a wood chipper with a mind of its own," he explains to *RPP*. "The data controllers set it out into a forest, but the wood chipper performs independently. It goes where it wants to go. Once you set it loose, there's little control over what it consumes. The challenge is to try to bring some accountability for it."

What many CEs may not realize is that their industry is already feeling the impact of AI, including in clinical decision support, research based on electronic health records, and fraud detection, Polsinelli shareholder Iliana Peters said during the webinar.

In most cases, the way that AI tools "learn" relies upon the processing of large volumes of data over long periods of time so that they can identify trends and recommend certain types of medical treatment.

Peters cited medical imaging, where AI is being used extensively as a clinical decision support tool. Similar to autonomous vehicles, however, it is important to remember that if AI applications malfunction, a person is at risk of physical harm, she warned.

With the increased expectations that AI will soon play a significant role in the health care sector, it is vital that CEs understand the regulatory frameworks surrounding the privacy and security of health data in order to guide their management of BAs that are providing AI services, she said.

According to Peters, the most common HIPAA-related issues that CEs must account for when contracting with AI vendors are related to data aggregation and data deidentification.

Under HIPAA's privacy provisions, data aggregation is the act of a BA combining protected health information

from multiple CEs in order "to permit data analyses that relate to the health care operations of the respective [CEs]."

Health information that does not identify an individual is not protected by HIPAA. Health information that has been deidentified, or made anonymous, is thus no longer subject to HIPAA protection. This so-called "safe harbor" requires removing identifiers, including names and addresses, of an individual, or their relatives, employers or household members.