THE
NATIONAL LAW REVIEW

# Artificial Intelligence: A Potential Cybersecurity Safeguard or Viable Threat to the Healthcare Industry?

Thursday, March 21, 2019

The healthcare industry is still struggling to address its cybersecurity issues as 31 data breaches were reported in February 2019, exposing data from more than 2 million people. However, the emergence of artificial intelligence (AI) may provide tools to reduce cyber risk.

AI cybersecurity tools can enable organizations to improve data security by detecting and thwarting potential threats through automated systems that continuously monitor network behavior and identify network abnormalities. For example, AI may offer assistance in breach prevention by proactively searching and identifying previously unknown malware signatures. By using historical data, these applications learn to detect malware issues even when such threats are not previously known. Utilizing these tools may prove more effective compared to conventional cybersecurity practices.


Article By Alaap B. Shah
Brian Hedgeman
Epstein Becker & Green, P.C.
Health Law Advisor

Communications, Media & Internet
Health Law & Managed Care
All Federal

Recently, government agencies have endorsed the use of AI as having tremendous potential moving forward. In December 2018, HHS launched a pilot that combined AI, automation, and blockchain technology. This pilot was used to create cost savings as well as design better contracts while also ensuring sensitive data was encrypted and secured within a cloud-based system. Additionally, in January 2019, the Department of Health and Human Services' shared services organization began building a contract vehicle, known as the Intelligent Automation/Artificial Intelligence (IAAI) contract, which offers "a host of automation and AI technologies and support services, including robotic process automation, machine and supervised learning and machine," to help other agencies integrate AI technologies into their workflows. Yet, certain lawmakers continue to express concern regarding appropriate and ethical use of AI.

Though AI is having a transformative effect on the healthcare industry relative to cybersecurity, there are still serious concerns regarding the technology. First, some AI tools could be used maliciously by criminals to threaten digital and physical security. External threats may train machines to hack systems at human or superhuman levels. Secondly, organizations relying too heavily on AI may fail to hire sufficient specialized security personnel to properly manage and oversee cybersecurity operations. For instance, a 2018 Ponemon report provided that 67 percent of IT and security professionals believed that automation was "not capable of performing certain tasks that the IT security staff can do" and roughly 55 percent believe automation cannot "replace human intuition and hands-on experience." Thus, poorly implemented and managed AI could result in greater risk.

Given the nascent state of AI in cybersecurity, entities should approach adoption of AI with caution. Further, successful implementation and use of AI should be predicated on first establishing policies and procedures for managing cyberrisk. Organizations should continue to maintain a team of highly skilled security personnel to oversee the implementation and use of AI tools and be on hand to make critical, real-time decisions where automation cannot resolve a cybersecurity issue. O, brave new world….