COSMOS
Navigate the Compliance Universe

# Compliance Today - October 2020
# Monitoring for privacy compliance with the use of AI in healthcare organizations

By Robin Singh, MSL, CCEP-I, HCCP, CFE, GIAC (US privacy)

**Robin Singh** (robin@whitecollar.org) is Group Senior Regulatory Affairs and Risk Management, Abu Dhabi Government – Healthcare Sector, Abu Dhabi, United Arab Emirates.

- linkedin.com/in/whitecollarinvestigator

The artificial intelligence (AI) healthcare space, by 2021, according to an Accenture study, is slated to reach $6.6 billion.[1] AI is continuing to play key roles across sectors and has emerged as an invaluable tool in healthcare. While the benefits of AI are many in healthcare, a lot of debate centers around the increasing use of AI in healthcare and, consequently, data privacy concerns.[2]

According to an IBM Security study, a single health record breach costs as much as $408, which is almost three times more than what data breaches cost in other industries.[3] A healthcare provider who has 2,500 records potentially could face a million-dollar loss for a data breach.

## AI in healthcare: Benefits

AI applications in healthcare are used primarily to analyze the association between treatment/prevention protocols and patient outcomes. AI programs find application in wide-ranging practices in healthcare, including diagnosis, personalized medicine, drug development, treatment protocol development, and patient care and monitoring.

AI can potentially improve the accuracy of diagnosis and treatment and help providers prioritize care on patients who require it the most. AI helps translate scientific discovery to actual practice and care, providing access to high-quality healthcare in remote rural settings.

## AI and data privacy regulations

The key regulation concerned with data privacy in healthcare is the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[4] The federal law establishes safeguards for protected health information (PHI), regulating the use and disclosure of PHI; rights of individuals in terms of PHI; and physical, administrative, and technical security safeguards that have to be implemented to protect PHI. HIPAA also mandates notification obligations when there is a breach of PHI.[5] In Europe, the General Data Protection Regulation (GDPR) covers data privacy in healthcare as well.[6]

The American Medical Association (AMA), in June 2018, released a statement on augmented intelligence policy in healthcare.[7] According to a board member of AMA, Jesse M. Ehrenfeld, technology provides “a unique opportunity to ensure that augmented intelligence is used to benefit patients, physicians, and the broad health care community.”

The AMA, according to the statement, will look to not only leverage digital health to set augmented intelligence-related priorities in healthcare but to integrate physician perspectives toward design, development, and implementation of augmented intelligence in healthcare.