COSMOS
Navigate the Compliance Universe

Ethikos Volume 32, Number 1. January 01, 2018
What happens when advances in technology raise the ethical bar?

By Nick Culbertson

Nick Culbertson (nick@protenus.com) is Chief Executive Officer and Co-Founder at Protenus in Baltimore, MD.

- www.protenus.com

The HIPAA Privacy Statute and related interpretive regulations—together known as the Privacy Rule—create a federal set of rights for patients to their protected health information. The rule translates to a simple premise: That the only person who can access your medical information is you.

As an exceptions statute, the Privacy Rule starts with a broad prohibition against the use or disclosure of protected patient information, unless the use or disclosure meets one or more exceptions. Most obviously, anyone providing medical treatment, such as your doctor, fits within the treatment exception to this broad prohibition. The Privacy Rule's counterpart—the HIPAA Security Rule—requires organizations to audit access to patient data to ensure that such accesses are proper. Advances in artificial intelligence (AI) make it possible for healthcare compliance professionals to audit each access to health data. To protect patient information, there may be an ethical obligation to do so.

Auditing electronic health records

Not too long ago, when health data was still largely limited to what your doctor wrote down in a paper chart, protecting patient information was relatively simple: Access to this information was generally limited to those directly responsible for patient care.

Today, health data has increasingly been converted to electronic format, and federal mandates, including Meaningful Use requirements, have encouraged the proliferation electronic health records. In turn, the number of people who have access to health data continues to increase. Through data sharing, interoperability, and health exchanges, nearly every health system employee, vendor, and business associate can access your digital health record.

At a large academic or regional medical center, it's not unusual for a day's work to generate more than 10 million actions inside an electronic medical record (EMR) system. Compliance officers have been doing their best to keep up by using the tools available: either reactive, manual audits in response to a suspected patient privacy violation or running routine reports (e.g., "Show me the top 10 most accessed patients"). Meant to identify the riskiest scenarios, these tools lack clinical context and ultimately, review an insignificant fraction of audit logs in an industry where 41% of all data breaches are attributable to insiders.

These approaches have been deemed acceptable, because health systems don't have the time or human capital to audit more. Unsurprisingly, patient privacy violations, such as the theft of hundreds of abortion records by an Ontario hospital employee taking part in an anti-abortion campaign,[1] continue to rise.

Yet, advances in technology, especially the ability of AI to analyze large amounts of unstructured data and serve up that analysis to augment human expertise, pose a new question for healthcare compliance officials: Is it

ethical to continue to audit only a portion of access to health data when AI makes it possible to protect patients by auditing every single one?

In other industries, AI is already replacing mundane, repetitive operations at an unimaginable scale, empowering subject-matter experts to focus in on the obvious patterns of anomalies. Law enforcement agencies use AI-powered fingerprint recognition software to identify criminals instead of flipping through massive binders of known prints. Credit card companies use AI to monitor our accounts for fraud, rather than having analysts review every single purchase. Instead, AI is used to elevate suspicious spending alerts for review, which allows the cardholder to confirm a purchase, and reduce overall fraud in a consumer population that would otherwise be unlikely to act if asked to review every purchase manually.

Yet, we are still having healthcare compliance officers manually review a mere fraction of accesses to some of our most sensitive patient data.