Google-Ascension deal comes as concerns rise on use of health data

NOV 14, 2019

Kevin B. O'Reilly
News Editor

What's in the news: Google and the 2,600-hospital Ascension health system are collaborating on an effort—dubbed Project Nightingale—that puts identifiable patient data in the hands of the tech giant's engineers for use in projects on machine learning (ML) and augmented intelligence (AI), often called artificial intelligence.

Google and Ascension say the activities, first reported by Rob Copeland of The Wall Street Journal, are covered by a business associate agreement, which is a long-standing, and legal, way for health care providers to share identifiable data with third parties under the Health Insurance Portability and Accountability Act (HIPAA).

The third parties may only use the data for certain purposes and must protect it as HIPAA requires. Failure to do so can result in direct liability for the business associate. The Department of Health and Human Services' Office of Civil Rights has announced that it will seek to learn more to ensure that HIPAA protections were fully implemented.

Why it matters to patients and physicians: This headline-grabbing collaboration comes as serious questions about the future of patients' data privacy take the foreground in ways that the AMA is urging doctors, patients and policymakers to take very seriously.

This much is clear: Patient privacy cannot be retrieved once it's lost. That's why the AMA has made protecting patient health data in the digital age a top priority. Above all, patients must feel confident that their personal health information will remain private. Preserving patients' trust is critical. The AMA *Code of Medical Ethics* offers extensive advice on privacy, confidentiality and medical records.

Anxiety around third parties, particularly technology giants, accessing and using patient health information is at an all-time high due to multiple reports on how Facebook, Google and other companies are getting their hands on this data without patients' knowledge or informed consent.

While HIPAA permits clinicians to share health care information with certain parties without a patient's consent, physicians must be responsible stewards of how patient data is disclosed. The patient-physician relationship is strengthened when patients are aware of and involved in decisions about how their information is used and disclosed.

The Google-Ascension deal raises additional questions about whether patients should be better informed about how their information is shared within the "HIPAA umbrella," whether business associates should be permitted to use patient data received through business associate agreements to build AI or ML tools that can be commercialized for later use, and whether patients should have to specifically consent to permit their data to be used to build AI or ML algorithms in the first place.

When patients learn that big tech, payers, or data brokers are commoditizing their data without their knowledge and consent—even if legally permissible—it can damage trust between patients and clinicians, particularly among populations whose data has historically been used for research without consent.

What's next: The Office of the National Coordinator for Health IT (ONC) and the Centers for Medicare & Medicaid Services (CMS) are expected to soon finalize rules pertaining to health information technology that will have a significant impact on the exchange, access and use of all health care data.

As proposed, the rules would shift the paradigm from permitting data sharing to required data sharing—including with third parties who would be under no obligation to keep the information private.

The rules focus on using advanced programming interfaces (APIs) and apps to provide patients with access to their complete medical record—a fundamental right that can improve the overall effectiveness of care.

The AMA fully supports patient access to the medical record and notes that it can improve the overall effectiveness of care. It points out, however, that by virtue of patients using apps to gain information, apps' developers will gain access to the information, too.

Patients and doctors should be aware that there are other emerging technologies in which health data is not covered by HIPAA. Mobile app developers and data brokers have relatively free reign to do with it what they wish, including using it or selling it for commercial gain.

Patients may not realize that their genetic, reproductive health, substance-use disorder, mental health, and familial information can be used to limit access to health, life insurance, or be disclosed to employers. Safeguards are needed that define the digital boundary between security and exploitation, and it's the reason why collaboratively developed guidelines for privacy and other elements of these apps were released earlier this year.

Compliance with the mHealth app guidelines can provide a level of assurance that an app delivers value to patients, physicians and other users. The guidelines were developed by Xcertia, a nonprofit founded by the AMA and other major health and technology organizations.

The AMA has called on ONC and CMS to ensure that certified APIs check whether apps connecting to an electronic health record adhere to industry-recognized development guidance such as Xcertia's guidelines, transparency statements and best practices, and whether the app provides a model privacy notice to patients. This information would help provide a minimal amount of transparency to patients about how a health app will use their health information.

Regulators should take note that the Google-Ascension deal—which includes parameters around how data can be used—has caused intense public scrutiny. As proposed, CMS and ONC's rules do not have any such parameters. The AMA believes that ONC and CMS should not finalize their proposals without including an attestation framework, at a minimum. It is possible to empower access while promoting privacy and transparency—patients deserve both.