COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 6. June 11, 2020 Amid New Privacy Principles, Doctors Seek HIPAA Expansion to 'Restore Trust'

By Theresa Defino

Spurred by concerns over contact tracing and, apparently, telehealth resulting from the COVID-19 pandemic and fearful of elements of new interoperability rules doctors say may go too far, the American Medical Association (AMA) has released a multipart group of "privacy principles" it said are needed to ensure the "sacred trust at the heart of the physician-patient relationship" remains and is strengthened.[1] AMA would give patients a private right of action, under some circumstances, and allow the government to go after individuals in a company for privacy violations—two changes from current-day HIPAA.

The principles would apply to organizations and providers that are not now subject to HIPAA and give a look into what AMA views as essential when it comes to privacy protections. App developers and others may want to review them to understand growing concerns.

AMA aims to actively engage members of the White House, Congress, federal agencies and industry stakeholders to adopt the principles and use them as the foundation for "discussions on the future direction of regulatory guardrails that are needed to restore public confidence in data privacy protections," it said.

"Recent events have highlighted how critical it is to have clear rules of the road with respect to data use. There is unprecedented reliance on remote care technologies, like telehealth, to help people avoid leaving their homes during the COVID-19 pandemic. But both patients and clinicians are justified in questioning how platforms will secure and protect the information exchanged during the virtual visits," AMA said in its announcement. "Similarly, many private and public efforts are underway to collect, use, and disseminate public health surveillance data to help inform public health officials and policymakers about the spread of the novel coronavirus. These efforts are critically necessary but must address questions about how best to handle the data both during collection and once the pandemic has subsided."

According to information AMA provided in response to questions from *RPP*, the principles document, issued May 11, has actually been under development since last spring—long before there was a pandemic or increasing use of telehealth.

Concern For Upcoming Regulations

AMA "saw movement in the regulatory landscape on the HIPAA front," including "questions from the administration about forcing covered entities to disclose information with third parties not bound by HIPAA, *RPP* was told. Association officials "submitted a comment letter in response to that Request for Information."[2] AMA also commented on the interoperability proposed rule, recently issued in final form.[3]

"If individuals aren't sure their information will be protected, they won't engage with new technologies and tools designed to help them (including apps designed to facilitate consumer-directed exchange of health information)," AMA told *RPP.*

Comments from AMA President Patrice Harris indicate longer-standing concerns.

"Patients' confidence in the privacy and security of their data has been shaken by repeated technology sector scandals and the wired economy's default business model that quietly gathers intimate glimpses into private lives—often without patient knowledge, consent or trust," she said. "As a result, patients are less willing to share information with physicians for fear that technology companies and data brokers will have full authority over the use of their indelible health data. Unfortunately, recently finalized federal regulations will make this more likely to happen."

The regulations are not mentioned in the principles themselves, and AMA's announcement spoke of "boosting the guardrails" around private information.

Speaking more generally, Harris said the principles "set a framework for national protections that provide patients with meaningful control and transparency over the access and use of their data."

More Types of Data Would Be Protected

AMA believes that "preserving patient trust is critical if digital health technologies are to facilitate an era of more accessible, coordinated, and personalized care. To restore confidence in data privacy and security, the AMA privacy principles promote individual rights, equity and justice, corporate responsibility to the individual, applicability and federal enforcement," said Harris. "The delicate balance between privacy and data protection on the one hand, and the protection of public health on the other, presents a number of challenges. The AMA's privacy principles provide a meaningful framework to guide data collection efforts, privacy legislation, and public health plans to help ensure that steps we take now will not unfairly and disproportionately impact vulnerable populations down the road, but rather will instill trust in the systems we establish to help keep people safe and healthy."

The statement to *RPP* noted that previous AMA documents address "information handled by clinicians," but that the association "wanted to create principles that extrapolated the AMA's values about privacy and applied them to the non-HIPAA setting."

The action is part of "the theme of ensuring there are constraints and protections for health information exchanged outside of HIPAA." In other words, as the principles state, they "apply to entities other than those already considered covered entities under HIPAA."

RPP also asked how the principles were being received, a question that wasn't addressed. "We've sent the principles directly to agency and Congressional officials engaged in privacy matters and policy-making," the statement said.

AMA noted that the principles "take into consideration that some data historically not considered 'personal' may in fact be personally identifiable (e.g., IP addresses, advertising identifiers from mobile phones). Accordingly, the Principles' use of the term 'data' includes information that can be used to identify an individual, even if it is not descriptive on its face."

Third parties that "access an individual's data should act as responsible stewards of that information, just as physicians promise to maintain patient confidentiality," AMA asserted. The principles "also call for robust enforcement of penalties for violation of rights to help patients develop and maintain trust in digital health tools, including the use of smartphone applications (apps) to access their own health information."

The principles have sections on individual rights, equity, entity responsibility, applicability and enforcement.

New privacy legislation should apply to organizations that "use, transmit, and disclose data, including HIPAA

business associates, with exceptions for HIPAA-covered entities given their obligations under existing HIPAA regulation," AMA said.

It is not drawing the line at health care firms, saying "different organizations, technologies, sectors" would have to comply with the new requirements.

Individuals Could Bring Suits

Under AMA's plan, the Federal Trade Commission (FTC) would enforce regulations for this new group of organizations, and, like with HIPAA, state attorneys general would be able to also bring cases. But, unlike HIPAA, AMA is calling for individuals to have a private right of action in the event that federal and state authorities fail to bring enforcement.

AMA said organizations have a "duty to maintain the confidentiality" of information and that they must disclose what is being collected, the purpose and with whom it will be shared; collect only "the minimum amount of information needed for a particular purpose"; and establish "protocols for retaining information for operational or regulatory compliance needs."

Additionally, entities would be "prohibited from using health data to discriminate against individuals, including creation of 'risk scores' that could hinder patients and their families from receiving health, disability, or life insurance; housing; employment; or access to other social services."

The principles call for Congress to fund the FTC to "investigate violations of an individual's privacy protections, with a report back to Congress identifying investigation outcomes and trends." AMA is also calling for legislation to expand Section 5 of the FTC Act "to include 'manipulative', 'abusive', and/or 'coercive' behaviors (i.e., behaviors that aren't outright deceptive or causing significant harm, but nevertheless designed to convince people to act against their best interest for the benefit of the entity—for example, dark patterns)."

FTC Would Have Broad Authority

AMA would also have Congress pass legislation giving FTC rulemaking authority, "specifically including the ability of FTC to define:

- "Unfair data processing practices (e.g., processing biometric or geospatial data that are not required for use of the app);
- "Additional safeguards for certain categories of information (contemplates future-gazing scenarios like human augmentation, cloning, etc.);
- "Boundaries of data systems;
- "Minimum privacy and security standards for products that process or use an individual's data (can help with privacy/security being built into the design of apps/products—known as 'privacy by design');
- "The minimum data elements needed for particular purposes;
- "To the extent appropriate, narrowly delineated exceptions to data deletion rights;
- "Mitigating and aggravating factors for establishing fine/penalty amounts (for example, penalties would be steeper for reckless disregard and knowing/willful conduct). FTC should have authority to impose penalties on both the entity and its officers.

- "Matters related to patient consent (how to define, what is informed and meaningful, etc.)."

Regarding consent, AMA officials said they "firmly believe that 'all or nothing' consent is meaningless and would not support such consent acting as a safe harbor from an entity's responsibilities under the statute and regulations."

In extending the HIPAA concept of minimum necessary, AMA said entities "should only collect the minimum amount of information needed for a particular purpose, in accordance with regulation and/or federal guidance. For example, a weather app may need general location data (e.g., zip code) but not precise location data (e.g., GPS coordinates)."

AMA expressed a hope that there would be "enhanced transparency around the use of business associates in health care, particularly now that entities not traditionally associated with health care are more active in the health care industry."

1 American Medical Association, "AMA issues new principles to restore trust in data privacy," news release, May 11, 2020, https://bit.ly/37jTj4l.
2 Jane Anderson, "HHS Looking for Input on Changes to Privacy Rule Affecting Care Coordination," *Report on Patient Privacy* 19, no. 1 (January 2019), https://bit.ly/30jdoGi.
3 Jane Anderson, "Final HHS Information Blocking, Interoperability Rules Released," *Report on Patient Privacy* 20, no. 5 (May 2020), https://bit.ly/2UjBPjg.