AMA health data privacy framework

AMA Privacy Principles

In the digital age, we continue to learn that personal health information is not truly private. Social media platforms, wearable fitness trackers and apps to manage pregnancy and mental health all collect health data that can be shared for advertising purposes and, when combined with medical records and other consumer information, allow for profiling and discrimination.

The AMA seeks to ensure that as health information is shared—particularly outside of the health care system—patients have meaningful controls over and a clear understanding of how their data is being used and with whom it is being shared. Above all, patients must feel confident that their health information will remain private. Preserving patient trust is critical.

Rapid growth in the range and volume of digital patient data beyond the confines of the HIPAA framework merits legislative attention. While more direct action should be taken in the near-term, without clear legislative guardrails, public trust will crumble in the face of repeated scandals and so undermine the potential for digital health to facilitate an era of more accessible, coordinated, and personalized care.

The AMA's Privacy Principles (PDF) seek to provide guidance on what these guardrails should include. They are derived primarily from AMA House of Delegates policy, and address (1) individual rights; (2) equity; (3) entity responsibility; (4) applicability; and (5) enforcement. These Principles will help the sector as we collectively work to ensure greater transparency and controls around data sharing.

Privacy

Health care information is one of the most personal types of information an individual can possess and generate. As the exchange of medical information between patients, physicians and the care team (also known as 'interoperability') improves, protecting an individual's privacy preferences and their personally identifiable information becomes even more important. The first step in creating a "privacy framework" is placing the patient first. Any individual or company seeking to access a patient's most confidential medical information must comply with federal and state law and develop or have an established trusted relationship with the patient. Moreover, citizens deserve a full and open

discussion of exactly who wants their private medical information and for what purpose. Only then may the true balancing of interests take place.

The AMA's approach to privacy is governed by our Code of Medical Ethics and long-standing policies adopted by our policymaking body, the House of Delegates, which support strong protections for patient privacy and, in general, require physicians to keep patient medical records strictly confidential. These policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the patient-physician relationship.

Patients' Health Information

Patients having access to their complete medical record is a fundamental right and can improve the overall effectiveness of care. Empowering patients, physicians, and the care team with useful and actionable information contributes to the quadruple aim—enhancing patient experience, improving population health, reducing costs, and improving the work life of health care providers. The importance of an accurate, usable, and complete medical record for care coordination is clear. Still, it is critical (and increasingly challenging) to balance access to a patient's longitudinal record with privacy. It is important that changes to state and federal laws do not erode protections meant to keep medical information private.

Without appropriate safeguards, patients' data could become a commodity. Patients' digital medical records are 50 times more valuable than financial information. Health data can provide a wealth of information for marketers or be sold and exchanged by data brokers—impacting insurance coverage, access to care, or resulting in employment discrimination. A loss of privacy may also affect an individual's behavior due to embarrassment or stigma. Keeping the patient at the center of care requires steadfast adherence to their rights to privacy.

Where Federal Health Data Policy Meets Privacy

Most personal health information exchanged between health care providers is governed by federal regulation. The Health Insurance Portability and Accountability Act (HIPAA) establishes guardrails for the sharing and use of patient health information. Generally, physicians and hospitals may share patient information without explicit patient consent for treatment, payment, and business operations reasons. HIPAA regulations are mainly "permissive" in that they allow but don't *require* the sharing of health information. This helps balance the need to share health information while holding HIPAA Covered Entities (CEs) accountable for the privacy and security of that information.

Two recently-proposed federal rules pertaining to health information technology and patient

information are poised to impact the exchange, access, and use of all electronic medical records. While there are elements in both rules that deserve support, there are also several problems—particularly when it comes to patient privacy. As proposed, the rules would shift the paradigm from permitting data sharing to requiring that data be shared—including with third parties and non-HIPAA CEs who would be under no obligation to keep the information private.

> **"The proposed rules are complicated, intertwined and may result in a patient's information being shared with third parties in a way that patient didn't foresee or want."**
>
> **—AMA Immediate Past President Barbara L. McAneny, MD**

The AMA wholeheartedly supports the right of patients to receive their medical information using smartphone applications, but is concerned about the lack of safeguards to ensure that patients understand what they are consenting to when they grant permission to an app to access their information. These apps share sensitive health information with third parties, often without an individual's knowledge. Much of this information can end up in the hands of data brokers and be used or sold for advertising and marketing. Data being used in this way may ultimately erode patients' privacy and their willingness to disclose information to their physicians.

As a first step to address this issue, the AMA is calling for controls to be instituted that establish transparency as to how health information is being used, who is using it, and how to prevent the profiteering of patients' data. To help provide a minimal amount of transparency to patients about how a health app will use their health information, the federal movement should implement a basic privacy framework requiring certified EHR vendor APIs to check an app's "yes/no" attestations to:

- Industry-recognized development guidance
- Transparency statements and best practices
- A clear privacy notice to patients

The AMA also has identified how the rules conflate a payer's desire for data with a clinician's need to access, exchange, and use health information. The rules will empower payers to demand more information than is needed, whether for regulatory compliance or other purposes. Physicians who deny a payer's request for this information may be accused of information blocking—regardless of whether the request is fully warranted.

"Historically, payers have only had access to clinical information when necessary for payment," Dr. James Madara, AMA's CEO and Executive Vice President stated in a letter to Department of Health and Human Services (HHS). Physicians take data stewardship very seriously. Removing physicians' ability to safeguard patient data could have "negative downstream consequences for patients and physicians" that would delay needed care, Dr. Madara writes. Payers could use the information

blocking proposals to demand patients' medical information and circumvent a physician's clinical decision-making.

Further, payers could use the proposals to request direct access into a physician's EHR. This raises significant concerns about payer overreach, increased prior authorization, and patient profiling—potentially limiting coverage and access to care, and causing an intrusion on physician medical decision-making. The AMA is requesting that the federal government prohibit payers from using these proposals to place additional contractual demands on physicians and impose meaningful penalties for payer noncompliance with this new prohibition. The AMA is also requesting that the federal government restrict payers from conditioning physician participation in a plan based on whether a doctor will grant the payer electronic access to the practice's EHR.

The AMA has provided several recommendations to strengthen medical data privacy and improve federal health information technology policy. Recent letters to the federal government include:

- Comment Letter to the Federal Trade Commission (FTC)
- Comment Letter to the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC) proposed information blocking rule
- Comment Letter to the Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services (CMS) proposed interoperability and patient access rule
- Testimony to the FTC
- Comment Letter to the Department of Health and Human Services' (HHS) Health Insurance Portability and Accountability Act (HIPAA) request for information
- Comment Letter to National Institute of Standards and Technology (NIST)