

## AMA Privacy Principles

As Congress continues discussions around federal privacy legislation, the AMA seeks to ensure that resulting privacy law protects the sacred trust at the heart of the physician-patient relationship. Specifically, the AMA is working 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.

These principles, derived primarily from AMA HOD policy, will serve as the foundation for AMA advocacy on privacy. They are meant to apply to entities other than those already considered covered entities under HIPAA—in other words, physicians generally would not be subject to additional regulation. 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.

The Principles provide individuals with rights and protections from discrimination and shift the responsibility for privacy from individuals to data holders other than HIPAA-covered entities (collectively referred to in this document as entities). In other words, third parties who access an individual's data should act as responsible stewards of that information, just as physicians promise to maintain patient confidentiality. 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.

Individual Rights:

- 1. Individuals have the right to know exactly what data of theirs an entity is accessing, using, disclosing, and processing—and for what purpose—at or before the point of collection.
- 2. Individuals have the right to control how entities access, use, process, and disclose their data, including secondary (and beyond) uses.
- 3. Individuals should be notified within a reasonable period of time following a material change in the entity's data access, use, disclosure, and processing practices.
- 4. Individuals have a right to direct entities to not sell or otherwise share data about them.
- 5. Individuals and entities should be able to protect and securely share pieces of information on a granular, as opposed to a document, level.
- 6. Individuals have a right to direct an entity to delete their data across the entity's ecosystem of services, including when the entity goes out of business or is bought out by another entity (with potential narrowly delineated exceptions, as determined by regulatory bodies and consistent with stakeholder input.
- 7. Individuals have the right to access and extract their data from a platform in a machine-readable format.
- 8. Individuals should have the right to know whether their data will be used to develop and/or train machines or algorithms. The opportunity to participate in data collection for these purposes must be on an opt-in basis.
- 9. Individuals should have a private right of action against entities that are subject to these requirements if the FTC and/or state Attorney General declines to pursue enforcement.
- 10. Privacy rights should be honored unless they are waived by an individual in a meaningful way, the information is appropriately de-identified (using techniques that are demonstrably robust, scalable, transparent, and provable), or in rare instances when strong countervailing interests in

© 2020 American Medical Association. All rights reserved.



public health or safety justify invasions of privacy or breaches of confidentiality and, in such case, to the minimum extent necessary.

- 11. Disclosures of an individual's data should be limited to that information, portion of the medical record, or abstract necessary to fulfill the immediate and specific purpose of disclosure.
- 12. Individuals who access their medical records using apps should have mechanisms to annotate but not change—the copy of the record they hold. These mechanisms should track who made the annotation, when, how, and why.

Equity:

- 1. Privacy protections should promote equity and justice.
- 2. Health care information is one of the most personal types of information an individual can possess and generate—regardless of whether it is legally defined as "sensitive" or protected health information under HIPAA—and individuals accessing, processing, selling, and using it without the individual's best interest at heart can cause irreparable harm.
- 3. Individuals should be protected from discrimination, stigmatization, discriminatory profiling, and exploitation occurring during collection and processing of data, and resulting from use and sharing of data, with particular attention paid to minoritized and marginalized (vulnerable) communities. Similarly, individuals should be protected from discrimination, stigmatization, profiling, and exploitation based on inferences drawn from a refusal to use or cessation of use of an app or digital health tool.
- 4. Because low-income individuals and other vulnerable populations have fewer resources and tools at their disposal to effectively assert their privacy rights, purchase technology with the most advanced and up-to-date privacy and security technology, and recover from harmful invasions of privacy, privacy frameworks (legal or otherwise) must advance policies to benefit individuals of all income levels. For example, the AMA would not support a policy in which paid apps provided greater privacy protections than free apps.
- 5. Law enforcement agencies requesting medical information should be given access to such information only with a court order and if the law enforcement entity has shown, by clear and convincing evidence, that the information sought is necessary to a specific, legitimate law enforcement inquiry; that the needs of the law enforcement authority cannot be satisfied by non-identifiable health information or by any other information; and that the law enforcement need for the information outweighs the privacy interest of the individual to whom the information pertains. Any applicable legal requirements for law enforcement access to medical information imposed by federal, state, or local laws shall apply in addition to this principle.
- 6. Employers and insurers should be barred from unconsented access to identifiable medical information to assure that knowledge of sensitive facts does not form the basis of adverse decisions against individuals, such as non-coverage of stigmatized health conditions.
- 7. Privacy legislation should provide robust and comprehensive protections against genetic discrimination and misuse of genetic information.

Entity Responsibility:

- 1. All entities that maintain an individual's health information should have an obligation or "duty of loyalty" to the individual, including the duty to maintain the confidentiality of that information.
- 2. An entity must disclose to individuals exactly what data it is collecting and the purpose for its collection. Such information should not be used for a materially different purpose than those disclosed in the notice at the point of collection of such information. For example, an entity that collects location data to provide weather should not use that data for advertising.



- 3. 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).
- 4. Entities should establish and make publicly available a data retention policy with established protocols for retaining information for operational or regulatory compliance needs.
- 5. Entities should be required to disclose to individuals what specific elements of data they collect, why, how often, for what purpose, and specifically with whom they are sharing the data.
- 6. Privacy policies should be written to promote understanding by individuals with elementary school levels of reading comprehension. Terms should be clearly defined and unambiguous. For example, statements such as, "We may share this data with our partners to improve quality" are vague and should not be permitted.
- 7. Entities should 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.
- 8. Entities should make their de-identification processes and techniques publicly available.

## Applicability:

- 1. Privacy legislation should apply to entities that access, use, transmit, and disclose data, including HIPAA business associates, with exceptions for HIPAA-covered entities given their obligations under existing HIPAA regulation. We believe this framework would lead to 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.
- 2. Local, state, and federally sponsored registries, as well as medical specialty-run registries, should be deemed in compliance with new privacy legislation if they establish a Data Governance Council. The Data Governance Council must include patient representatives and establish practices around sharing registry data. Note that some health conditions (such as HIV or substance use disorder) may have additional, more restrictive privacy safeguards, including through state law. This principle is not intended to replace those protections.
- 3. Privacy legislation should be adaptable to many different organizations, technologies, sectors, and uses to promote competition. It should also be scalable to organizations of all sizes and be platform- and technology-agnostic and customizable.
- 4. We recognize the potential need for accommodations for small businesses in certain scenarios, but overall privacy principles should apply to them as they do to larger businesses. For example, an entity with fewer than 10 employees may not need a full-time privacy officer but must still be able to satisfy responses to individuals with questions about the entity's data practices.
- 5. Privacy legislation should promote data access needed for narrowly delineated medical or public health research or quality improvement and accreditation activities by clinicians and researchers, including open access to appropriate machine-readable public data, while prioritizing the development of a culture that informs individuals about the potential benefits and risks of sharing data with external partners, explicit communication of allowable use with periodic review of informed consent, and protections against using data to deny or limit access to coverage.

## Enforcement:

- 1. Individuals should not be responsible for costs of enforcement unless they are exercising their private right of action (in permitted instances where the Federal Trade Commission (FTC) and the individual's State Attorney General (AG) do not enforce).
- 2. Federal privacy legislation should serve as a federal floor, not a ceiling.
- 3. Legislation should not weaken any state's laws or regulations regarding privacy.

© 2020 American Medical Association. All rights reserved.



- 4. State Attorneys General (AGs) should be permitted to bring an action in federal court to enforce these requirements on behalf of their states' residents.
- 5. Federal privacy legislation should authorize funds for FTC to investigate violations of an individual's privacy protections, with a report back to Congress identifying investigation outcomes and trends.
- 6. Federal legislation should 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).
- 7. Legislation should provide the FTC with Administrative Procedures Act (APA) rulemaking authority, specifically including the ability of FTC to define:
  - a. Unfair data processing practices (e.g., processing biometric or geospatial data that are not required for use of the app);
  - b. Additional safeguards for certain categories of information (contemplates future-gazing scenarios like human augmentation, cloning, etc.);
  - c. Boundaries of data systems;
  - d. 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");
  - e. The minimum data elements needed for particular purposes;
  - f. To the extent appropriate, narrowly delineated exceptions to data deletion rights;
  - g. Matters related to patient consent (how to define, what is informed and meaningful, etc.). We 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; and
  - h. 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.