Health.
Virtually.
Everywhere.

The ATA's Health Data Privacy Principles

The protection of patient data is prerequisite for connected care and a core principle for our organization. The ATA supports efforts to ensure telehealth practices meet standards for patient safety, data privacy, and information security, while advancing patient access and building awareness of telehealth practices.

Consistency:

Regulatory consistency across industries is paramount to protecting consumer privacy while simultaneously mitigating compliance, complexity and financial costs for U.S. companies. A federal policy would offer consistency and is preferable to a state-by-state approach. However, as states adopt privacy statutes and regulations, an effort to establish uniformity with existing federal and other state standards would reduce both complexity of compliance and confusion for consumers and companies alike. Privacy laws should allow for innovation and the advancement of technology-assisted care. Personal health information used in telehealth and virtual care platforms, systems, and devices should be secured and protected from misuses and inappropriate disclosures.

Definition of Consumer Health Data:

State law and policy should define consumer health data (and other terms commonly used to characterize personally identifiable health care information) by adopting the same language that defines protected health information in the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA:

State consumer privacy laws should be consistent with and not exceed HIPAA's standards to the greatest extent possible, to ensure that patient protections are not contingent on whether the entity is HIPAA-covered. HIPAA-covered entities and their business associates should be exempt from state privacy laws. HIPAA is a proven, decades-old data privacy framework. Requiring HIPAA-covered entities to adhere to additional layers of state privacy laws would negatively impact their ability to deliver services, increase compliance costs, and stymie innovation.

Consumer Rights:

Consumers should be entitled to meaningful, accessible, and actionable rights, including: a right to notice, a right to access, a right to correct, a right to portability, a right to delete so long as these rights are consistent with other medical record retention laws and contains an exception for when data may be required to defend against legal claims or to comply with legal obligations. Notices should include all categories of data, processors, and other third parties the data controller is working with. Notices should also indicate that consumers can receive specific information regarding their personal information upon request. At the same time, all covered entities should be allocated a reasonable amount of time to comply with various consumer requests, including a consumer's request to delete data.

Consumer Consent, Sale of Data & Opt-Out:

Consumers should be provided clear and conspicuous disclosures on what data is collected, how it will be used, and a how to opt-out of processing for purposes of (a) targeted advertising, (b) the sale of personal data; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. If applicable, disclosures should also clarify whether any data will be shared or sold for any purpose outside what is required to provide the service requested by the consumer. What constitutes the sale of data should be clearly defined, and the sharing of any sensitive data should require explicit disclosure to and consent from the patient. Sensitive data should be defined as personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis, sexuality, or citizenship or immigration status; genetic or biometric data processed to identify individuals; and precise geolocation data.

Enforcement:

State Attorneys General should be empowered to take enforcement action when privacy laws are violated. However, private rights of action should not be included in data privacy policy because they can lead to a lack of clarity, result in frivolous lawsuits, and result in out-of-court settlements that exacerbate legal uncertainty.

ata®
Health.
Virtually.
Everywhere.

www.americantelemed.org

Adopted by the ATA Policy Council: June 2023
Approved by the ATA Board: July 2023