AHIMA Policy Statement on Health Information held by HIPAA non-covered entities

AHIMA's Position:

AHIMA supports the use of policy to address existing privacy, confidentiality, and security gaps in the protection of health information held by Health Insurance Portability and Accountability Act (HIPAA) non-covered entities. Federal privacy and security baseline standards should be developed for the protection of health information held by data holders[1] outside of the scope of HIPAA. Standards should take into account the data holder's size, scope, activities, and sensitivity of the health information collected, used, and maintained as well as risk of inappropriate disclosure and misuse.

Health information (HI) professionals have extensive expertise in ensuring the privacy, confidentiality, and security of an individual's health information. AHIMA has developed a set of privacy principles below to help inform its ongoing advocacy efforts in this area. The principles envision the privacy, confidentiality, and security of health information throughout its entire lifecycle. In this context, AHIMA intends "health information" to refer to "electronic health information" as defined at 45 CFR 171.102.[2] The principles are intended to be technology agnostic and adaptable to differing technologies and platforms. The principles are also intended for data holders that are not covered by HIPAA and are not intended to supersede, alter, or affect entities currently covered by HIPAA. To ensure the confidentiality, privacy, and security of individuals' health information, AHIMA believes that policy must:

1. **Guarantee individuals' access to their health information.** Policy must guarantee that individuals have access to their health information regardless of where it travels.

2. **Improve accountability.** Policy must ensure that data holders develop, document, communicate, assign, and are held accountable for their privacy policies and procedures.

3. **Enhance communication and transparency.** Policy must ensure data holders communicate what information will be collected and maintained and generally how the data may be processed and disclosed, including whether data will be sold or commercialized.

4. **Limit the collection, use, and disclosure of health information.** Policy must ensure data holders limit the amount of health information collected, used, and disclosed to the minimum necessary.

---

[1] The National Committee for Vital and Health Statistics (NCVHS) defines a "data holder" as "an inclusive term referring to entities that design and maintain proprietary databases and algorithms, sell data products, or design and build apps and devices that capture, transmit or use health data."

[2] "Electronic health information" means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in the designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity. EHI does not include psychotherapy notes (as defined in 45 CFR 164.501) or information compiled in reasonable anticipation of, or for use in a civil, criminal or administrative action or proceeding.

5. **Ensure the accuracy and integrity of health information.** Policy approaches must encourage the completeness, accuracy, and integrity of health information.

6. **Prioritize the protection of health information** against various privacy and security risks, including breaches and unauthorized disclosures.

7. **Address health information retention concerns.** Policy should safeguard that health information is retained no longer than necessary by data holders.

8. **Facilitate disposition and destruction of health information.** Policy should facilitate the proper disposition and destruction of health information.

9. **Assign appropriate oversight and enforcement responsibilities.** Policy must clearly designate and adequately fund oversight and enforcement responsibilities.

Background:

The state of health data privacy in the US is rapidly evolving as the digitization of the healthcare sector accelerates. Historically, the US has followed a patchwork approach, applying a sector-specific approach to data privacy versus a single data privacy regime.[3] As a result, absent sector-specific requirements, certain technologies, applications, products and services, are not bound by or required to abide by robust privacy protections.

HIPAA governs health privacy in traditional healthcare settings.[4] However, an increasing number of consumer-facing technologies, applications, products, and services that access, produce and manage health information are not bound by or required to abide by the rules established under HIPAA because they are not considered "covered entities" or "business associates." Rather, the privacy practices of such applications, products and services are generally regulated by state law and/or the Federal Trade Commission (FTC) Act. However, unlike sector-specific data protections, the FTC Act does not prescribe specific privacy requirements but rather prohibits unfair or deceptive acts or practices in or affecting commerce.[5] This kind of oversight does not provide the same type or level of protections for consumers as HIPAA, which offers such safeguards as notice of privacy practices; security; restrictions on the sale, use, and reuse of PHI by third parties; and the individual right of access.

Key Points:

AHIMA offers the following policy recommendations to ensure that entities not covered by HIPAA are held accountable for the privacy and security of health information.

Individual Access:

- Individuals have the right to access their health information regardless of where that information travels. Individuals have the right to access, at a minimum, their health information as defined in 45 CFR 164.501.

[3] Terry, Nicolas, "Assessing the Thin Regulation of Consumer-Facing Health Technologies," *Journal of Law, Medicine, & Ethics*, 48 S1 (2020): 94-102.
[4] Id.
[5] 15 USC § 45(a)(1).

Accountability:

- Data holders should implement both initial and ongoing workforce development training to educate employees engaged in the data processing[6] of health information to ensure they are trained to perform privacy-related duties. Third parties (e.g., service providers, partners, etc.) should also be held accountable for training associated with the performance of privacy-related duties.

- Data holders should document employees' and third parties' commitment to adherence to privacy policies and procedures.

- Date holders should be held accountable and face consequences for failure to adhere to the policy recommendations set forth in this document.

Communication/Transparency:

- Data holders should clearly and conspicuously communicate what information will be collected and maintained and generally how the data may be processed and disclosed.

- Data holders should be required to make their privacy policy available in plain language before the individual shares any health information. The privacy policy should contain categories of health information it collects, processes, maintains and discloses; practices of the data holder including an articulated basis for the collection, processing, maintenance and disclosure of such information; and how individuals may exercise their rights under the policy and the law. The privacy policy must also be provided to the individual via a process that is concise, clear, intelligible, and easily accessible.

- Policies, processes, and procedures should be in place for receiving, tracking, and responding to complaints, concerns, and questions from individuals about a data holder's organizational privacy policies and practices.

- Individuals must have the opportunity to clearly communicate their privacy preferences. Policies, processes, and procedures should be in place to enable an individual's privacy preferences and requests, including a reasonable mechanism to revoke consent.

Collection, Use and Disclosure

- Collection, access, use, disclosure and maintenance of health information must be limited to no more than what is reasonably necessary to accomplish the intended purpose.

- Consent to collect, access, disclose and maintain health information should be sought whereby an individual makes an informed decision to share their information and the choice is recorded and maintained. Consent should be revocable at any time.

[6] The National Institute of Standards and Technology (NIST) defines "data processing" as "the collective set of data actions (i.e., the complete data life cycle, including but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission and disposal. https://www.nist.gov/sites/default/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf, https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

- Access to health information by an individual's employer should not be permitted unless an individual authorizes a data holder to do so or is required by law.

- Data holders should not sell an individual's health information without the express consent of the individual.

- Secondary uses of data must be disclosed to the individual with an option to opt-in, except as required by law.

- Collection, access, use, disclosure, and maintenance of health information is expressly prohibited for purposes of discrimination, stigmatization, discriminatory profiling, and/or exploitation.

Accuracy and Integrity[7]

- An individual has the right to inspect health information related to him or her and to have such data amended or completed.

- Individuals have the right to request that a data holder amend health information about them so long as the health information is maintained by the data holder. A data holder may deny an individual's request for amendment if it determines that the health information that is the subject of the request was not created by the data holder (unless the individual provides a reasonable basis to believe that the originator of health information is no longer able to amend or correct the health information or the health information is accurate and complete).

Protection

- Using privacy and security industry standard best practices, health information should be protected against risks such as loss or unauthorized access, destruction, use, modification, or disclosure of data.

- Data holders should notify an individual following discovery of a breach of the individual's health information in a timely manner, in accordance with the Federal Trade Commission (FTC)'s Health Breach Notification Rule.

Retention

- Data holders should maintain health information no longer than necessary while taking into account legal, regulatory, fiscal, and operational requirements. Data holders should develop a health information retention schedule specifying what information must be retained and for what length of time.

Disposition and Destruction

- Data holders should in the normal course of business regularly provide secure and appropriate disposition of health information no longer required to be maintained by applicable laws and the organization's policies.

[7]The knowledgeable, contextual, secure, and appropriate creation and use of health data.

- Destruction of health information should be conducted in accordance with industry standard best practices after the appropriate retention period.

Oversight and Enforcement

- Oversight and enforcement of entities not covered by HIPAA should be assigned to a single federal agency, such as the FTC. Adequate resources including funding and tools; a clear congressional mandate must also be provided to ensure appropriate oversight and enforcement.

Current Situation:

In 2019, Senator Maria Cantwell (D-WA) introduced the Consumer Online Privacy Rights Act (COPRA) and Senator Roger Wicker (R-MS) introduced a discussion draft of the United States Consumer Data Privacy Act (USCDPA). The House Energy and Commerce Committee also released a draft bipartisan privacy bill at the end of 2019 that sought to lay out a comprehensive privacy framework.

With the advent of the COVID-19 pandemic, new questions have arisen as to how health information may be leveraged for public health purposes including surveillance, contact tracing and immunization, including how technology may be leveraged to enhance public health capabilities. However, such issues underscore the continued need to address confidentiality, privacy and security gaps in the governance of health information.

AHIMA will actively advocate for and participate in development of privacy policies to ensure appropriate protections are put in place when health information is gathered and shared by entities not covered by HIPAA.