DoD's Structure under HIPAA and its Impact on Various DoD Components

Introduction

Pursuant to the Health Insurance Portability and Accountability Act (HIPAA), the Department of Defense (DoD) designated itself as a single affiliated covered entity in DoD Health Information Privacy Regulation, DoD 6025.18-R. In this regulation, the DoD specifically defined the Military Health System (MHS) to only include DoD components that are health plans and health care providers that conduct standard electronic transactions (i.e., components that meet the definition of a HIPAA covered entity). The DoD 6025.18-R also applied HIPAA to DoD components acting as business associates, including components engaged in non-covered functions that otherwise act as business associates. In doing this, the DoD functionally structured itself like a hybrid entity. DoD's intent is to only apply HIPAA to components that would in and of themselves need to comply with HIPAA and components that act as business associates. DoD components that solely provide non-covered functions and do not act as a business associate are not regulated by HIPAA.

Definitions

Definitions for terms noted with an asterisk (*) were abbreviated for purposes of this Information Paper; however, full definitions can be found in DoD 6025.18-R at DL 1.1.

Business Associate*: A person who:

On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information or other function or activity regulated by this Regulation; or

Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

Common Control: Exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common Ownership: Exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Covered Entity: A health plan or a health care provider who transmits any health information in electronic form in connection with a transaction covered by DoD 6025.18-R, e.g. ACS X12N837 health care claims, ASC X12N 270/271 eligibility inquiries and responses, and the electronic forms of other transactions. In the case of a health plan administered by the DoD, the covered entity is the DoD Component (or subcomponent) that functions as the administrator of the health plan. To the extent this Regulation prescribes duties to be performed by covered entities, the term refers only to DoD covered entities. All covered entities of the MHS (including both health plans and health care providers) are designated as a single covered entity. Not all health care providers affiliated with the Armed Forces are covered entities; among those who are not are providers associated with Military Entrance Processing Stations (MEPS) and Reserve components practicing outside the authority of military treatment facilities (MTFs) who do not engage in electronic transactions covered by the Regulation.

Covered Functions: Those functions of a covered entity the performance of which makes the entity a health plan or health care provider.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of protected health information (PHI) outside the entity holding the information.

Health Care Provider: Any MTF or dental treatment facility. This includes garrison clinics and such facilities in a military operational unit, ship, or aircraft, and any other person or organization outside of such facilities' workforce who furnishes, bills, or is paid for health care in the normal course of business. This term includes occupational health clinics for civilian employees or contractor personnel.

Health Care Component: A component or combination of components of a hybrid entity designated by the hybrid entity in accordance with the HIPAA regulations.

Health Plan*: Any DoD program that provides or pays the cost of health care, unless exempted.

Hybrid Entity: A single legal entity: (1) that is a covered entity; (2) whose business activities include both covered and non-covered functions; and (3) that designates health care components in accordance with the regulations.

Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual; and is created or received by a health care provider, health plan, or employer; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Military Health System (MHS): All DoD health plans and all DoD health care providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by, the Defense Health Agency (DHA), the Army, the Navy, or the Air Force.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, including name, social security number, date and place of birth, mother's maiden name, biometric records, and any other personal information which is linked or linkable to a specified individual.

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium. PHI excludes individually identifiable health information in employment records held by a covered entity in its role as employer. PHI does not include health information of persons deceased more than 50 years.

Use: With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Discussion

Organizational Structures for HIPAA Compliance

HIPAA regulates covered entities, which include health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a standard transaction set forth in the regulations. HIPAA also regulates business associates, which are entities that provide a service to a covered entity and require PHI to perform the service. Unless otherwise structured, an organization regulated by HIPAA is deemed a single covered entity, and the entire organization must comply with HIPAA. This means that all components of the organization, including any components that do not engage in covered functions (also known as non-covered components) must be trained and adhere to all of HIPAA's privacy, security, breach notification, and enforcement standards for safeguarding PHI. Covered entities that are legally separate, but under common ownership and control, are able to designate themselves as a "single affiliated covered entity." In a single affiliated covered entity, all of the affiliated covered entities function as one HIPAA covered entity, sharing the same HIPAA policies, procedures, and notice of privacy practices.

When an organization includes both covered and non-covered components, however, HIPAA provides an option for the organization to structure and declare itself a "hybrid entity." In a hybrid entity, only the organization's covered components and components acting as business

associates of covered components are identified as "health care components" and required to comply with HIPAA. This enables the organization to implement HIPAA in a manner that reduces unnecessary exposure to administrative obligations, legal risks, and unintended costs.

The definition of a hybrid entity created some confusion when HIPAA was enacted by suggesting that only a "single legal entity" can designate itself a hybrid entity. HIPAA does not address whether legally separate but affiliated entities, under common ownership and control, can designate themselves as a hybrid entity. However, the Department of Health and Human Services (HHS), the agency mandated to implement and enforce HIPAA, has shown through its own organizational designation as a hybrid entity that an organization made up of legally separate but affiliated entities, under common ownership and control, may designate itself a hybrid entity.

HIPAA requires that any component within a hybrid entity that would, in and of itself, meet the definition of a covered entity or business associate must be designated a heath care component and be required to comply with HIPAA. Thus, the health care components within a hybrid entity must include health plans, health care clearing houses, and health care providers engaging in standard electronic transactions, as well as any non-covered components within the hybrid entity that function as business associates. The health care components must comply with HIPAA and adhere to all of its protections, individual rights, and administrative obligations. In addition, individually identifiable health information created or received by the health care components is considered PHI that must be protected by HIPAA. Components not designated as health care components because they neither conduct covered functions nor act as business associates are not regulated by HIPAA. Likewise, individually identifiable health information created or received by or on behalf of such non-covered components is not PHI and is not protected by HIPAA. Non-covered components, however, must still adhere to other applicable regulations, including the Privacy Act, and provide safeguards and individual rights regarding PII.

In a hybrid entity, components that are not designated as health care components may not have access to PHI held by a covered component, unless the HIPAA Privacy Rule permits such disclosure or access. In addition, the health care components must protect their electronic PHI (ePHI) as required by the HIPAA Security Rule as if the covered components and non-covered components were separate and distinct entities. If a workforce member performs duties for both covered and non-covered components, then the member may not use or disclose PHI created or received in the course of or incident to the member's work for the covered component in a manner prohibited by HIPAA. For example, a health care provider who works in an MTF that is a covered component and also works as a researcher within a non-covered component cannot disclose or access PHI from the MTF when working as a researcher within the non-covered component. Instead, the provider/researcher must protect the PHI maintained by the MTF and request access to the PHI for the purpose of research in accordance with the HIPAA Privacy Rule requirements.

DoD's Structure for HIPAA Compliance

Due to a lack of clarity when HIPAA was enacted as to whether affiliated covered entities could designate themselves as a hybrid entity, DoD declared its affiliated covered entities within the MHS as a single covered entity. However, DoD functionally structured itself as a hybrid entity. DoD defined the MHS to include DoD components that would otherwise meet the definition of a covered entity only for purposes of HIPAA. *See*, the definition of MHS at DoD 6025.18-R at C3.2.1 and as set forth in the definitions above. DoD specifically designated its components that include health plans and health care providers that conduct standard electronic transactions as covered components regulated by HIPAA. *See*, DoD 6025.18-R at C3.2.3. The DoD 6025.18-R also clearly applied to DoD components acting as business associates, including DoD non-covered components that otherwise act as business associates. *See,* DoD 6025.18-R at C3.4.1. DoD's intent has always been to only apply HIPAA to its components that would, in and of themselves, need to comply with HIPAA and its components acting as business associates. DoD has never intended for components that solely provide non-covered functions and that do not act as business associates to be regulated by HIPAA.

Future updates to DoD's HIPAA implementation regulations may ultimately provide further clarification by designating the DoD as a hybrid entity. However, the current regulations, in essence, structure the DoD as a hybrid entity and allow it to function accordingly. Thus, a potential revision to DoD's HIPAA implementation regulations to designate the DoD as a hybrid entity would not change the regulations' requirements for covered components as currently written. Rather, such a revision would clarify that only covered components and DoD components acting as business associates, including non-covered components that act as business associates, are governed by HIPAA.

The examples below demonstrate the impact of DoD's structure as a hybrid entity on various covered and non-covered components within DoD:

- The Armed Forces Health Surveillance Branch (AFHSB) is a component within DoD that functions as a public health authority. By structuring itself as a hybrid entity, DoD carved out its specific covered components required to comply with HIPAA, such that non-covered components not otherwise acting as business associates are not required to comply with HIPAA. As the AFHSB is a non-covered component that does not act as a business associate, it is not subject to HIPAA. The AFHSB, however, is still required to comply with other applicable laws, such as the Privacy Act, and with obligations pertaining to PII.

- Researchers that work in DoD covered components must comply with HIPAA's standards, even if they are not themselves health care providers engaging in standard electronic transactions. This means that they must safeguard the PHI created, accessed, or received in the course of their research in accordance with the HIPAA privacy, security, breach notification, and enforcement standards. To the extent that a researcher performs duties

for both DoD covered and DoD non-covered components, then the researcher may not use or disclose PHI created, accessed, or received in the course of or incidental to the researcher's work for the covered component in a manner prohibited by HIPAA. Regardless of whether a researcher works in a DoD covered or non-covered component, the researcher must request PHI from a covered component in accordance with the HIPAA Privacy Rule's research provisions before a covered component is able to share access to or disclose PHI for research purposes (e.g., a researcher cannot use PHI obtained in the course of providing health care for research purposes without first receiving appropriate HIPAA Privacy Rule approval from an Institutional Review Board (IRB) or HIPAA Privacy Board).

Resources/References

HIPAA, 45 CFR Parts 160 and 164.

DoD Health Information Privacy Regulation, DoD 6025.18-R, January 2003.