

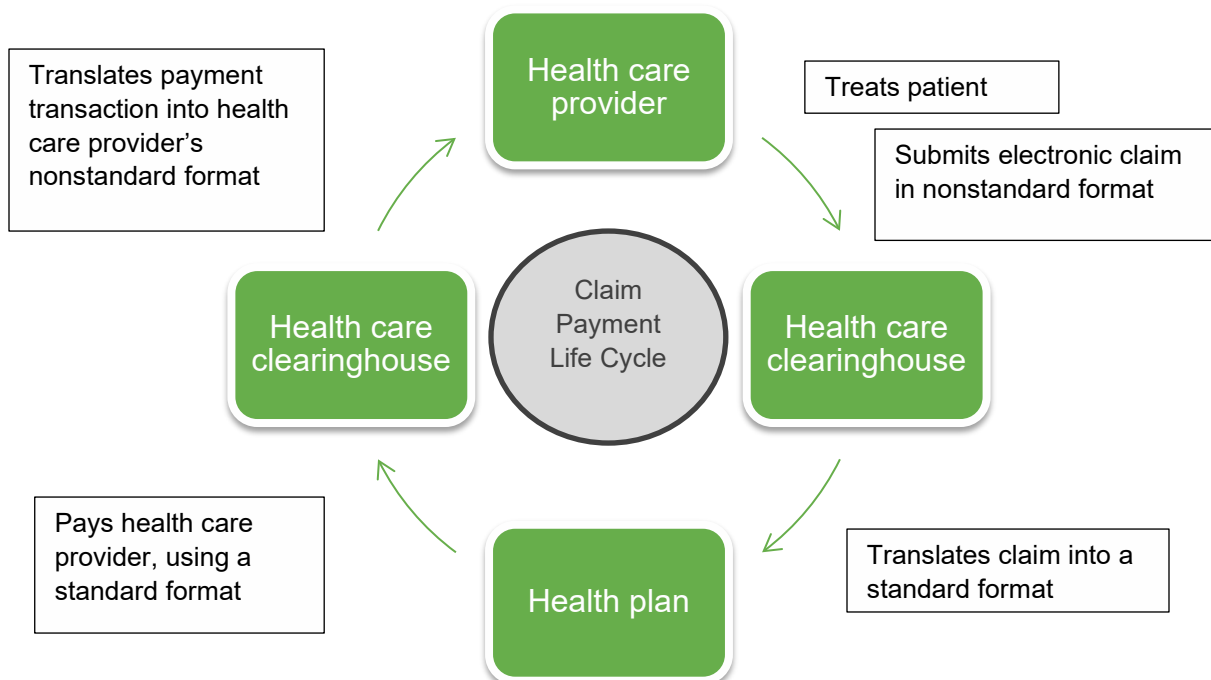



HYBRID ENTITY
Read Me First

In the early 1990s, health plans attempted to standardize the claim payment life cycle - claims submission, processing and payment - in the health care system. This effort sought to gain efficiencies, improve quality and reduce costs. At the time, electronic health information was shared in a multitude of formats with varying industry-imposed requirements.¹ Realizing that industry needed federal action to mandate standardization, Congress passed the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), in 1996. One of HIPAA’s primary objectives is to achieve “administrative simplification” in the claim payment life-cycle.²

HIPAA mandates that the U.S. Department of Health and Human Services adopt national standards for the electronic transactions that take place between health plans and health care providers in the claim payment life cycle. It also regulates the exchanges of information that occur with health care clearinghouses, that often sit between health plans and health care providers. Health care clearinghouses standardize and reformat electronic transactions, making them readable to the recipient organization.³

The following figure⁴ reflects health care providers, health plans and health care clearinghouses’ claim payment life cycle.





Congress recognized that as a part of this process, electronic health information must be secured. Accordingly, Congress mandated that security standards be developed to safeguard this information. And, in order to prevent the erosion of privacy over time by this explosion of electronic health data, Congress directed that privacy protections be established.⁵

Even though security and privacy concerns around electronic health data were not the driving force behind HIPAA, there are now hundreds of pages of privacy and security rules, guidance, and FAQs. HIPAA is complex and challenging in its application; public health does not always fit neatly into the HIPAA paradigm. This toolkit addresses the question of how HIPAA applies to public health. It also identifies the hybrid entity option as a useful and beneficial HIPAA classification. This hybrid entity toolkit offers FAQs, use cases, fact sheets, a policy template, a reference table, an issue brief and resources.

HIPAA does not apply to all organizations or individuals that collect, use, or share health information; nor does it apply all health information. To determine its applicability to a health department, first determine whether the health department is a covered entity.

What is a covered entity?⁶

Covered entities are regulated by HIPAA. There are three types of covered entities:

- *Health care providers*, such as doctors, hospitals, clinics, psychologists, dentists, chiropractors, nursing homes, laboratories and pharmacies . . . *but only if they bill or perform related standard transactions electronically*
- *Health plans*, such as health insurance companies, health maintenance organizations, Medicaid programs and Children's Health Insurance Plans
- *Healthcare clearinghouses*, which translate and standardize electronic transactions in the billing process (unlikely to be found within a health department)

The common link between each of these covered entities is that they participate in the claim payment life cycle and are required to utilize standard electronic transactions.

Public health is covered by HIPAA where it provides health care, such as in a clinic environment, or in its laboratory, and submits a claim or other transactions electronically to a health plan, or a clearinghouse. If a health department offers grant funded screening or immunizations, for example, and does not submit an electronic claim to a health plan for payment, it is not a covered entity. Additionally, a health department is covered by HIPAA when it operates a health plan, such as Medicaid. Coverage under HIPAA hinges on whether the health department is engaging in electronic claims submission, processing and payment.

If a health department provides a service that makes it a covered entity, it is likely that it has other organizational components that provide support. These components function like business associates; the next step is to determine whether the health department has any business associate components.

What is a business associate?⁷

Business associates are regulated by HIPAA. A business associate component is part of a hybrid entity:

- That performs services for any of the components that are covered entities or other business associates and,
- Involves the use or sharing of protected health information (PHI).

Examples include: public health attorneys, privacy officers, security officers, accountants, managers, leadership, information technologists, accounts receivable and billing clerks.



What information does HIPAA protect?

HIPAA regulates PHI, which is typically record level data. PHI is information, including demographic information:

- In any form: written, electronic or oral
- Created or received by a health care provider, health plan, employer, or health care clearinghouse
- Relating to past, present or future
 - Physical or mental health status or condition
 - Provision of health care
 - Payment for provision of health care
- And, that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.⁸

De-identified health information is not PHI.

What does the HIPAA Privacy Rule do?

HIPAA regulates PHI held by covered entities and their business associates. The HIPAA Privacy Rule has two primary objectives:

- Address covered entities' use and sharing of PHI, ensuring that it is properly protected and,
- Establish standards for individuals' privacy rights to understand and control how their PHI is used and shared.⁹

To ensure that PHI is properly protected, HIPAA prohibits the use or sharing of PHI, unless the HIPAA Privacy Rule requires or allows it, or the individual who is the subject of the information has authorized the use or sharing.¹⁰

HIPAA does not intend to impact use or sharing of PHI for traditional public health activities, which it recognizes as a matter of national priority.¹¹ In fact, HIPAA specifically permits covered entities to share PHI with public health for the purpose of "reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions."¹²

What options does HIPAA offer for coverage?¹³

Generally, these options are utilized by health departments:

- Option 1: *Single covered entity*. If a health department offers any services that make it a covered entity, it should decide whether to remain fully and completely covered by HIPAA; this is the default coverage classification. Being fully covered by HIPAA means that those activities that fall outside of HIPAA, such as the traditional public health activities, are covered by HIPAA. Or,
- Option 2: *Hybrid entity*. The health department may decide to generally restrict HIPAA to only those covered entity and business associate components that are legally required to be regulated by HIPAA, such as a clinic or a Children's Health Insurance Plan. [Read More](#).

Which option is best for a health department?

- Generally, it is best for a health department to restrict HIPAA coverage by becoming a hybrid entity.
- Becoming a hybrid entity ensures that HIPAA does not impact traditional public health activities. It also ensures that associated data sharing is not limited by HIPAA and remains regulated by state and local law.
- Becoming a hybrid entity reduces compliance burden. Further, it shields traditional public health activity components from HIPAA's breach notification requirements. [Read More](#).

Becoming a hybrid entity requires several steps.

What does becoming a hybrid entity require?¹⁴

- Evaluate whether the health department is independent or is legally part of a larger organization.
- Determine which components are covered entities.
- Determine which components are business associates.

Adopt a hybrid entity policy that lists all of the components that are covered entities and business associates.¹⁵ [Read More](#).

SUPPORTERS



Robert Wood Johnson Foundation

Support for the Network provided by the Robert Wood Johnson Foundation. The views expressed in this document do not necessarily reflect the views of the Foundation.

This document was developed by Sallie Milam, JD, CIPP/US/G, Deputy Director, Network for Public Health Law – Mid-States Region Office, and reviewed by Denise Chrysler, JD, Director, Network for Public Health Law – Mid-States Region Office. The Network for Public Health Law provides information and technical assistance on issues related to public health. The legal information and assistance provided in this document does not constitute legal advice or legal representation. For legal advice, please consult specific legal counsel.

¹ Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule; Nass SJ, Levit LA, Gostin LO, editors. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington (DC): National Academies Press (US); 2009. 4, HIPAA, the Privacy Rule, and Its Application to Health Research (IOM 4). Retrieved from: <https://www.ncbi.nlm.nih.gov/books/NBK9573/> at p. 1.

² *Id.*

³ Centers for Medicare & Medicaid Services. (2017, July 26). *Transactions: Transactions Overview* (CMS Transactions). Retrieved from <https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html>. Congress also requires that all code sets and identifying numbers used in these transactions be standardized. HHS. (2017, June 16). *HIPAA for Professionals*. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/index.html>.

⁴ See, Conklin, A. "Healthcare Payment & Remittance Medical Banking - Best Practices," slide 6. Retrieved from www.ehcca.com/presentations/HIPAA9/4_05_1.ppt.

⁵ IOM 4 at 2; HIPAA for Professionals.

⁶ [45 CFR §§ 160.103, 164.104](#).

⁷ [45 CFR §§ 160.103, 164.105\(a\)\(2\)\(iii\)](#).

⁸ [45 CFR § 160.103](#).

⁹ HHS. (2013, July 26). *For Professionals: Summary of the HIPAA Privacy Rule*. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

¹⁰ *Id.*

¹¹ *Id.*

¹² HHS. (2003, April 3). *For Professionals: Public Health*. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html>.

¹³ [45 CFR § 164.103](#).

¹⁴ *Id.*

¹⁵ [45 CFR § 164.105\(a\)\(2\)\(iii\)](#).