



## HYBRID ENTITY FAQs

### Hybrid Entity FAQs

While the U.S. Department of Health and Human Services did not intend the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA) to cover traditional public health activities, HIPAA does regulate the provision of certain services that health departments might provide. For example, a health department may provide HIPAA covered health care services because it operates a hospital or a health clinic or electronically bills for testing services provided by the state public health laboratory. It may also operate a HIPAA covered health plan such as Medicaid or a State Children’s Health Insurance Plan.

When a health department provides HIPAA covered services, it is a covered entity and must ensure HIPAA compliance. A covered entity may limit HIPAA to those organizational components that are regulated by HIPAA. This is known as becoming a hybrid entity.

Becoming a hybrid entity enables a health department to carve out its traditional public health activities – disease or injury registry functions, vital events record functions, and conducting public health surveillance, investigations, or interventions – from HIPAA coverage. This election requires the covered entity to assess itself against HIPAA and to document the results in a written hybrid entity policy.

### The following FAQs provide an overview of HIPAA’s hybrid requirements:

---

#### QUESTION

#### ANSWER

---

**What is a hybrid entity?**

A hybrid entity is an organization that is:

- A single legal entity;
  - That is a covered entity;
  - That also provides non-covered services; and,
  - That adopts a *written* hybrid entity policy.
-

---

**What is a single legal entity?**

A single legal entity is the smallest *legally* recognized unit of the organization. Examples include:

- An independent or freestanding state health department
- A state umbrella agency, which operates a state health department and provides other services, such as mental health, environmental quality or human services
- An independent or freestanding local health department
- A municipality, which operates a local health department and provides other services, such as water supply, sewage collection and disposal, refuse removal, electricity and gas supply, municipal roads and storm water drainage, street lighting, municipal parks and recreation

---

**What is a covered entity?**

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 (very unlikely to be found within a health department)

If an organization is a covered entity, it may be described as providing covered services.

---

**What is a non-covered service?**

Non-covered services are those that are unrelated to performance as a health plan, health care provider or health care clearinghouse. HIPAA exempts:

- Traditional public health activities, where authorized by law, to collect or receive information for preventing or controlling disease, injury, or disability. This includes the reporting of disease and injury, and vital events, and conducting public health surveillance, investigations, and interventions
- Public health or government functions, where authorized by law, to receive reports of child abuse or neglect

HIPAA exempted services, such as traditional public health activities, are referred to as non-covered services.

---

**What is a hybrid entity policy?**

A written policy, in hard copy or in electronic media that identifies:

- Any component that would meet the definition of a covered entity; and,
- Any component that would meet the definition of a business associate, within a hybrid entity.

*Optional:* A health care provider that does not bill electronically may also be included. This is the only non-covered service that may be included.

---



<b>What is a business associate within a hybrid entity?</b>	<p>A business associate within a hybrid entity includes staff who perform services for any of the components that are covered entities or business associates, involving the use or disclosure of protected health information (PHI). Examples include:</p> <ul style="list-style-type: none"><li>• Public health attorneys, privacy officers and security officers</li><li>• Accountants, managers, leadership and information technologists</li><li>• Accounts receivable and billing clerks</li></ul>
<b>What is a component?</b>	<p>Because organizations' composition varies greatly, the term component is used to refer to any organizational subdivision. A component may be a bureau, office, division, program or unit. Covered entities have discretion in identifying and designating their components.</p> <p>For example, if health department's Bureau A is a fully covered entity, then health department must identify Bureau A as a covered entity component. However, if Bureau B has three divisions and Division 1 is a covered entity and Divisions 2 and 3 engage in traditional public health activities, the health department may elect to identify Division 1 from Bureau B as a covered entity component, instead of identifying the entire Bureau B as the covered entity component. A granular review of activities and services may allow a health department to more effectively limit HIPAA.</p>
<b>If an organization hasn't gone through the formalities of creating and adopting a written hybrid entity policy, can it still be considered a hybrid entity?</b>	<p>No. If the organization has not adopted a written hybrid entity policy, HIPAA treats it as a single covered entity. With a single covered entity, HIPAA applies to all components, including non-covered services, such as traditional public health activities.</p>
<b>How long must the hybrid entity policy be kept?</b>	<p>This policy must either be in writing or electronically recorded, and kept for six years or the date when it last was in effect, whichever is later.</p>
<b>If an organization becomes a hybrid entity, do the non-covered components, such as public health, still have to comply with all of HIPAA?</b>	<p>No. Becoming a hybrid entity prevents HIPAA from applying to non-covered services, such as traditional public health activities.</p>
<b>May a hybrid entity freely share PHI within the bounds of its legal entity?</b>	<p>No. The components that are covered entities or business associates must safeguard the PHI. They must treat the non-covered components the same as they treat an external party, with regard to sharing PHI.</p> <p>As an example, if a covered entity component, such as a clinic, wants to share PHI with a non-covered component, and the HIPAA Privacy Rule requires patient authorization for such disclosure to an external party, then the covered entity component – the clinic – must obtain patient authorization prior to sharing the PHI. If the clinic does not obtain patient authorization for the disclosure and HIPAA requires patient authorization, then HIPAA prohibits the disclosure.</p> <p>If the clinic wants to share PHI with a different non-covered component, such as public health, and public health is authorized by law to receive the information for preventing or controlling disease, injury, or disability, and</p>



---

	HIPAA does not require patient authorization, then HIPAA allows the disclosure.
<b>What kind of security must be put in place to protect the PHI held by a hybrid entity?</b>	The hybrid entity must comply with the HIPAA Security Rule to safeguard the PHI held by its covered entity and business associate components from disclosure to its non-covered components.
<b>May an employee work for both a covered entity component and a non-covered component of the same hybrid entity?</b>	Yes. However, the employee may not use or disclose any PHI created or received by the covered entity component in a way that violates the HIPAA Privacy Rule.
<b>If an organization chooses to be a hybrid entity, who is legally responsible for HIPAA compliance?</b>	The legal entity is responsible for ensuring HIPAA compliance.

---

For access to the HIPAA Privacy Rule and commentary concerning the hybrid entity classification, [please see the Hybrid Entity Regulatory Reference Table](#).

**SUPPORTERS**



Robert Wood Johnson Foundation

The Network for Public Health Law is a national initiative of the Robert Wood Johnson 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.