



HEALTH INFORMATION AND DATA SHARING
Issue Brief

An Overview on Conducting a HIPAA Hybrid Entity Assessment for Local Public Health Departments

Introduction

The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA) applies to many local public health departments (LHDs). This issue brief helps public health practitioners, and their attorneys understand how HIPAA applies to LHDs, the steps an LHD must take to become a HIPAA hybrid entity, and discusses how these decisions directly impact data sharing, operations, compliance burden, and risk.

Who or What is Covered by HIPAA?

Health plans, health care clearinghouses, and health care providers that generate and receive standard electronic transactions are covered by HIPAA¹ and are known as *covered entities*.² Examples of standard electronic transactions include: claims information and status, eligibility, enrollment, and coordination of benefits.³ An LHD that is also a health care provider but does not engage in any standard electronic transactions — for example, if it only provides free clinical services — is not covered by HIPAA.

Examples of HIPAA Covered Entities

COVERED HEALTH CARE PROVIDER	HEALTH PLAN	HEALTH CARE CLEARINGHOUSE
This includes providers such as:	This includes:	This includes a public or private entity that either processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction or receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data
Doctors	Health insurance companies	
Clinics	HMOs	
Psychologists	Company health plans	
	Certain government programs that pay for health care, such	

Dentists	as Medicare, Medicaid, and the military and veterans' health care programs	content for the receiving entity.
Chiropractors		
Nursing Homes		
Pharmacies		

...but only if they transmit any information in an electronic form in connection with a transaction for which United States Department of Health & Human Services (HHS) has adopted a standard.

Business Associates

There is an additional type of entity called a business associate. Business associate is defined within HIPAA as a person or entity who, on behalf of a covered entity, creates, receives, maintains, or transmits protected health information (PHI) for a function or activity regulated by 45 C.F.R. § 160, such as claims processing, data analysis, or utilization review.⁴ A business associate can also include an entity that provides legal, actuarial, management, administrative, and financial services. Like covered entities, business associates are HIPAA covered.⁵

What information is covered?

HIPAA regulates PHI, which is individually identifiable health information:

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) 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

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.⁶

PHI does not include certain education records, employment records, and records regarding a person who has been deceased for more than 50 years, even if these records may contain health information.⁷

If HIPAA covers an organization, it must comply with both the HIPAA Privacy and Security Rules, amongst other

requirements, for the PHI that it collects, creates, uses, discloses, retains, and destroys. PHI held by a health care provider may look similar to the health information held by an LHD that is not a covered entity, but they are not legally the same. HIPAA does not regulate the health information received by an LHD for traditional public health purposes, such as surveillance, if the LHD is not a covered entity. It is important to begin the analysis of whether HIPAA applies by first determining whether the entity is a covered entity or business associate, and then ascertain whether the information is PHI.

What is a hybrid entity?

HIPAA recognizes larger organizations such as LHDs may have some components that are required to be covered by HIPAA and some that need not be. For example, an LHD may provide clinical services, in addition to carrying out other public health activities such as disease surveillance and food and water safety (a permitted carve-out from HIPAA). The LHD is not required to make the entire organization subject to HIPAA. Instead, it can limit HIPAA's applicability to those covered components, such as clinical services, which are subject to HIPAA. The components subject to HIPAA are called "health care components". A single legal entity that offers both covered and non-covered services may elect to become a *hybrid entity*.⁸

Becoming a Hybrid Entity Can Facilitate Data Sharing

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

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

HIPAA prohibits the use or sharing of PHI unless the HIPAA Privacy Rule allows or requires it, or the individual or their personal representative authorizes it. HIPAA recognizes the importance of public health activities, and specifically permits covered entities to share PHI with a public health authority without authorization for the purpose of "preventing or controlling disease, injury, or disability."⁹

Becoming a hybrid entity is a policy option that has the potential to carve out non-covered traditional public health components, such as registries, surveillance programs, and inspection programs from HIPAA. Becoming a hybrid entity expressly limits HIPAA's application and may streamline the sharing of public health data. From an operational standpoint, it allows LHDs to share data with potentially greater ease as the public health components are no longer required to comply with HIPAA.



Becoming a Hybrid Entity is Key to Reducing Risk and Compliance Burden

Becoming a hybrid entity may reduce an LHD's HIPAA compliance burden, risk, and exposure. By simple numbers, the fewer components covered by HIPAA, the smaller the HIPAA regulatory footprint.

HHS' Office of Civil Rights (OCR) enforces the HIPAA Privacy and Security Rules' compliance requirements. One of the many requirements is workforce training on all policies and procedures.¹⁰ Unless the LHD is a hybrid entity, if a health department performs any HIPAA-covered functions, it must train all members of the workforce, many who never see or touch PHI, on HIPAA privacy and security measures.

HIPAA also requires performing complex risk assessments and drafting and implementing policies and procedures. The combined text of the HIPAA rules is over 100 pages, and there is also extensive guidance and commentary informing implementation.¹¹ Becoming a hybrid entity generally confines application of these complicated and lengthy rules to only those components that legally require it.

When there is a breach of PHI, HIPAA requires notification of affected individuals, HHS, and possibly the media, which is costly to the LHD in terms of financial and personnel resources.¹² (A breach is the acquisition, access, use, or disclosure of PHI in violation of the HIPAA Privacy Rule, which compromises the security or privacy of the PHI.) By becoming a hybrid entity, an LHD may reduce the chance of a HIPAA covered breach because it is likely fewer members of its workforce are accessing or disclosing PHI. LHDs should also be aware that even if HIPAA does not apply to the data that is breached, there may be a separate breach notification requirement under separate state or federal law.

Challenges with Becoming a Hybrid Entity


There are some operational challenges that need to be addressed when becoming a HIPAA hybrid. For example, the LHD must erect firewalls around the PHI held by the health care components and the health care components may not disclose PHI to a non-health care component (unless permitted to do so by HIPAA). The LHD must protect PHI with respect to another component of the LHD to the same extent it is required to do so under the HIPAA Security Rule if the health care component and non-health care component were separate legal entities. Also, if there are staff that work for both health care components and non-health care components, then they must not use or disclose PHI in their work for the non-health care component. An LHD should assess these potential challenges alongside the benefits of becoming a hybrid entity.

Begin with an Assessment

To become a hybrid entity, an LHD must assess which organizational components HIPAA covers. This assessment has two parts: (1) determination of the legal identity of the health department and (2) evaluation of services against HIPAA.

Legal Identity

The first step is to confirm the identity of the legal entity within which the LHD sits.¹³ Is the health department legally independent? Or, is it part of a larger organizational unit?



OCR provides limited guidance and states that a single legal entity is the smallest legally recognized unit of the organization. OCR offers the example of a single legal entity that is a manufacturing firm with a health clinic on-site, with the health clinic not separately incorporated. Both the manufacturing firm and the health clinic are part of the same corporation, which is the legal entity.¹⁴

Determining the legal entity that “owns” an LHD requires more research. There may be no governmental filing, akin to a private corporation’s articles of incorporation, that legally distinguishes an LHD from another government agency. Collaboration between public health practitioners and public health attorneys is key to determining the legal entity.

A local health department is “the governmental body serving a jurisdiction or group of jurisdictions geographically smaller than a state and recognized as having the primary statutory authority to promote and protect the public’s health and prevent disease in humans.”¹⁵ Local health departments may be locally governed; a local entity of a centralized state health department; or, a city, city-county, county, district, or regional health department.¹⁶ To determine the legal entity, it may help to review the state’s constitution, statutes, regulations, or any applicable executive orders to determine how units of local government are organized. If the law is unclear, review existing Attorney General opinions for guidance or consider requesting an opinion.

Also, it may be beneficial to review the charter that defines the organization, responsibilities, and authority.¹⁷ The charter functions as a “constitution” for the city or county. Identify and review all city and county codes, and any pertinent summaries and guidance, which pertain to the establishment of the health department.¹⁸ Some local governments give their health departments independence by charter or ordinance. An independent local health department is the single legal entity.

Additional Resources. If the law is unclear, consider the following questions:

1. Does your LHD have authority to sue or be sued in its own name?
2. Is control and supervision of your LHD vested within the department? Or is it vested within a broader organization, such as a city or an umbrella organization?
3. What is the degree of financial autonomy and the source of operating expenses for your LHD?¹⁹
4. What do relevant organizational charts and websites reflect?


If the LHD is an independent legal entity, the LHD should perform the HIPAA assessment across the entire health department. If the health department is embedded in a larger organization which is the legal entity, the HIPAA assessment must be performed across the larger organization.

The HIPAA assessment discussion below is framed with the LHD as the legal entity. It is equally applicable to the situation where the LHD is part of a larger organization which is the legal entity.

HIPAA Assessment

The HIPAA assessment requires identifying the health care components of an LHD that would be covered entities or business associates if they were separate legal entities. LHDs may have a mix of covered components (including business associates) and non-covered components.

The following example offers context to HIPAA terminology and the hybrid entity assessment process with



respect to an LHD:

An LHD's clinic provides health care services, such as immunizations and STI testing, to individuals and bills health plans electronically for those services. The clinic shares PHI with other divisions of the LHD, including the general counsel's office and accounting department. After undertaking the HIPAA hybrid entity assessment, the LHD identifies its clinic as a health care provider that bills electronically for services, which, were it a separate legal entity, would make it a covered entity under HIPAA, and its legal and accounting departments as business associates. Other components conducting disease reporting and public health surveillance are non-covered functions.²⁰ In this example, HIPAA does not apply to the non-covered components; these components are generally governed by state or local privacy and confidentiality laws, regulations, and policies.²¹ The LHD carves out the covered entity and internal business associate components, in this case the clinic and the legal and accounting departments and following the adoption of a hybrid entity policy, HIPAA only applies to these health care components.

Hybrid Designation Decision. If the assessment reflects that the LHD has any type of health care component, then by default HIPAA applies to the entire local public health department. This means that HHS could hold the entire LHD subject to the HIPAA standards, including components that if they were a separate legal entity, would not be covered by HIPAA, such as traditional public health components. Where the LHD has chosen the hybrid designation, it is important for the health department to take the necessary steps to become a hybrid entity.

Responsibilities of the Legal Entity

The legal entity that has chosen to become a hybrid entity has oversight and compliance obligations under HIPAA. For example, the legal entity must ensure that health care components do not use or disclose PHI in violation of HIPAA.²² Particular attention must be paid to confirm that sharing between the covered health care components and non-covered components does not violate HIPAA. Additionally, the legal entity must adopt the appropriate HIPAA privacy and security policies and procedures.

Finally, the legal entity is responsible for making certain that all related contracts, including business associate agreements and other organizational requirements, are in place.²³ Federal guidance suggests that the legal entity enter into contracts and conduct other organizational matters at its level, instead of at a lower level, such as with an individual health care component like a clinic.²⁴

Adoption of Hybrid Entity Policy

To officially become a hybrid entity, the legal entity must designate in writing or record electronically its components that perform covered functions as "health care components."²⁵ This includes all covered entity and business associate components.²⁶ Without this the LHD is not actually a hybrid entity and remains fully covered by HIPAA.²⁷ Legal entities must also retain this documentation for six years from its creation or the date when it was last in effect, whichever is later. Using the example directly above, the LHD must designate in writing the clinic and the legal and accounting departments as health care components.

Legal entities have the option of including health care providers that do not bill electronically in the hybrid entity policy.²⁸ Applying HIPAA coverage to these providers allows PHI sharing to be characterized as an

internal use and not an external disclosure. This could be advantageous in sharing PHI for health care operations with an internal health care provider that does not bill electronically and therefore is non-covered. In this limited situation, patient authorization is not required.²⁹ LHD's should carefully evaluate this potential advantage against increased regulatory burden, risk, and liability.

Review of the hybrid entity designation should occur whenever there is any change in organizational function or structure, applicable law, or in the way that PHI is collected, used, or disclosed.

Conclusion

HIPAA provides essential protections to PHI and helps promote trust that people's data remains confidential. However, an overbroad application of HIPAA at the entity level for LHDs can constrain data sharing and increase compliance burden and the risk of HIPAA-covered breaches. Identifying where HIPAA requires compliance in LHDs and making a hybrid entity designation may position LHDs to share data with greater ease, achieve improved HIPAA compliance, and reduce risk.

SUPPORTERS



Robert Wood Johnson Foundation

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

This update and revision was prepared by Meghan Mead, J.D., Acting Deputy Director Mid-States Region, Network for Public Health Law, with support from Marisa London, J.D./M.P.H. Candidate, 2025, University of Michigan Law School. The original publication was prepared by Denise Chrysler, J.D., Director, Network for Public Health Law – Mid-States Region and Sallie Milam, J.D., CIPP/US/G, Deputy 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 References to being "covered by HIPAA" also mean "covered function," "covered entity" and "business associate."

² Definitions and examples of each type of covered entity is provided in the next section.

³ COMMITTEE ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFORMATION: THE HIPAA PRIVACY RULE, *HIPAA, the Privacy Rule, and Its Application to Health Research in BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH* 153, 153 (Sharyl J. Nass, Laura A. Levit, & Lawrence O. Gostin eds., 2009), <https://www.ncbi.nlm.nih.gov/books/NBK9573/>.

⁴ Definitions, 45 C.F.R. § 160.103 (2013), <https://www.eC.F.R..gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-A/section-160.103>.

⁵ *Public Health*, U.S. DEP'T OF HEALTH AND HUM. SERVS., (April 3, 2003) <https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html>.

⁶ 45 C.F.R. § 160.103.

⁷ *Id.*

⁸ Definitions, 45 C.F.R. § 164.103 (2017), <https://www.eC.F.R..gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-A/section-164.103>.

⁹ 45 C.F.R. § 164.512(b).

¹⁰ Administrative requirements, 45 C.F.R. § 164.530 (2017), <https://www.eC.F.R..gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.

¹¹ The official version of the guidance can be found at 45 C.F.R. Parts 160, 162, and 164. *HIPAA for Professionals*, U.S. DEP'T OF HEALTH AND HUM. SERVS., (June 16, 2016), <https://www.hhs.gov/hipaa/for-professionals/index.html>.

¹² 45 C.F.R. § 164.400 *et seq.* (2017), <https://www.eC.F.R..gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>.

¹³ 45 C.F.R. § 164.103.

¹⁴ Health Care Component (Component Entities), 65 Fed. Reg. 82502 (Dec. 28, 2000) (to be codified at 45 C.F.R. 164.504), <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf?language=es>.

¹⁵ PUBLIC HEALTH ACCREDITATION BOARD, STANDARDS: AN OVERVIEW 4 (2011) <https://www.phaboard.org/wp-content/uploads/PHAB-Standards-Overview-Version-1.0.pdf>.

¹⁶ *Id.*

¹⁷ See, *What are Government Entities and Their Federal Tax Obligations?*, I.R.S. (Aug. 17, 2017), <https://www.irs.gov/government-entities/federal-state-local-governments/government-entities-and-their-federal-tax-obligations>.

¹⁸ Administrative requirements, 45 C.F.R. § 164.530 (2017), <https://www.eC.F.R..gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>.

¹⁹ See, *What are Government Entities and Their Federal Tax Obligations?*, *supra* note 17.

²⁰ Brian Kamoie & James G. Hodge, Jr., *HIPAA's Implications for Public Health Policy and Practice: Guidance from the CDC*, 119 PUB. HEALTH REPS. 216, 218 (2004), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1497612/pdf/15192909.pdf>.

²¹ Claire V. Broome, et al., *Statutory Basis for Public Health Reporting Beyond Specific Diseases*, 80(2) J. OF URBAN HEALTH: BULLETIN OF THE N.Y. ACAD. OF MED. i14, i17 (2003), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3456544/pdf/11524_2006_Article_190.pdf; ASSOCIATION OF STATE AND TERRITORIAL HEALTH OFFICES, INFORMATION MANAGEMENT FOR STATE HEALTH OFFICIALS: DATA SHARING WITH COVERED ENTITIES UNDER THE HIPAA PRIVACY RULE, A REVIEW OF THREE STATE PUBLIC HEALTH APPROACHES 7 (2004), https://biotech.law.lsu.edu/cdc/astho/29408_ASTHO.pdf.

²² Safeguard requirements, 45 C.F.R. § 164.105(a)(2)(ii) (2020), <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-A/section-164.105>.

²³ Responsibilities of the covered entity, 45 C.F.R. § 164.105(a)(2)(iii) (2020), <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-A/section-164.105>.

²⁴ Administrative Safeguards, 78 Fed. Reg. 5590 (to be codified at 45 C.F.R. 164.308), <https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf>.

²⁵ *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUM. SERVS., (Oct 19, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>; Organizational requirements, 45 C.F.R. § 164.105(c)(2)(iii) (2020), <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-A/section-164.105>.

²⁶ This is also known as designation of health care components. Definitions, 45 C.F.R. § 160.103 (2013), <https://www.eC.F.R..gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-A/section-160.103>.

²⁷ *Id.*

²⁸ 45 C.F.R. § 164.105(a)(2)(iii)(D).

²⁹ Uses and disclosures to carry out treatment, payment, or health care operations, 45 C.F.R. § 164.506(c)(4) (2017), <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.506>.