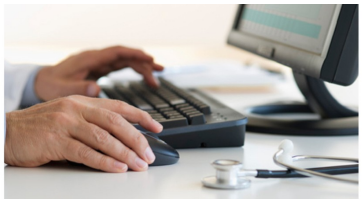
The Network for Public Health Law

Ideas. Experience. Practical answers.

HIPAA
Issue Brief

HIPAA Hybrid Entity Coverage Assessments

Introduction

The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), covers most health departments at the state and local levels. This issue brief aids public health practitioners and their attorneys to better understand how HIPAA applies to services a health department may provide, options for coverage under HIPAA, and how these decisions directly impact data sharing, compliance burden and risk. It also details the steps a health department must undertake if it wants to become a hybrid entity and restrict HIPAA coverage, as well as the safeguards it must put in place. This issue brief highlights changes in law and regulatory enforcement action that provide compelling reasons for health departments to update their HIPAA coverage assessments, even if they are already hybrid entities.

Background on HIPAA

In the early 1990s, health plans attempted to reduce costs by standardizing claims submission and payment processes in the health care system. Sharing electronic health information occurred in a multitude of formats, based upon varying industry-imposed requirements.[1] Realizing that industry needed federal action to mandate standardization, Congress passed HIPAA in 1996.

HIPAA mandates that the U.S. Department of Health and Human Services (HHS) adopt national standards for the electronic transactions that take place between health plans and health care providers related to payment for health care.[2] It also standardizes the exchanges that occur with health care clearinghouses that often sit between health plans and health care providers. Health care clearinghouses reformat electronic transactions, making them readable to the recipient organization.

Who is covered?

Health plans, health care clearinghouses and health care providers, that generate and receive standard electronic transactions, are covered by HIPAA[3] and are known as *covered entities*.[4] Standard electronic transactions include:

- Claims and encounter information

Payment and remittance advice
Claims status
Eligibility
Enrollment and disenrollment
Referrals and authorizations
Coordination of benefits
Premium payment[5]

These transactions trigger HIPAA coverage. If a health care provider has a means of receiving income that does not involve any of the above listed electronic transactions, such as grant funding or submission of paper claims, then the health care provider is not HIPAA covered.

Examples of HIPAA Covered Entities

HEALTH CARE PROVIDER	HEALTH PLAN	HEALTH CARE CLEARINGHOUSE
This includes providers such as:	This includes:	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.
Doctors	Health insurance companies	
Clinics	HMOs	
Psychologists	Company health plans	
Dentists	Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	
Chiropractors		
Nursing Homes		
Pharmacies		
...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.		

Businesses or persons that provide support services to a covered entity and process that entity's protected health information (PHI), are known as *business associates*. Examples of services include quality assurance activities, patient safety activities, legal services, actuarial services, personal health records and subcontractors. Like covered entities, business associates are HIPAA covered. [6]

Congress recognized that as a part of this process, electronic health information must be secured. Accordingly, Congress mandated the development of national security standards to safeguard this information. In order to prevent the erosion of privacy over time by this explosion of electronic health data, Congress also directed that privacy standards be established.[7]

What 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.[8]

PHI does not include education records, employment records and records regarding a person who has been deceased for more than 50 years.[9]

If an organization is covered by HIPAA, it must comply with both the HIPAA Privacy and Security Rules 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 a public health disease registry, but they are not legally the same. HIPAA does not regulate the health information received by public health for traditional public health purposes, such as surveillance. It is important to begin the analysis of HIPAA coverage at the organizational level and not with a comparison of the health information.

What is a hybrid entity?

Importantly, HIPAA recognizes that many organizations have complex missions with components that are covered by HIPAA and some that are not. These organizations are not required to make their entire organization subject to HIPAA. HIPAA provides flexibility and the choice to generally limit HIPAA regulation to those components that are actually covered by HIPAA. This process is known as becoming a *hybrid entity*.[10] A single legal entity that offers both covered and non-covered services may elect to become a hybrid entity.[11]

How are state health departments classified under HIPAA?

The Association of State and Territorial Health Officials (ASTHO) published a report reflecting how state public health departments classified themselves under HIPAA in 2004. [12] Information from this report is reflected below. In 2018, The Network for Public Health Law distributed a questionnaire to learn more about state and Washington DC's health departments' experiences with their HIPAA classifications. Updating the ASTHO report reflects that most state health departments that responded to the questionnaire or offered information via e-mail are hybrid entities.

HIPAA Coverage Classification 2004 and 2018

STATE	HIPAA CLASSIFICATION 2004	HIPAA CLASSIFICATION 2018	STATE	HIPAA CLASSIFICATION 2004	HIPAA CLASSIFICATION 2018
Alabama	Hybrid	Hybrid	**Montana**	Covered	Hybrid
Alaska	Covered	Covered	**Nebraska**	Covered	Covered
Arizona	Hybrid	Hybrid	**Nevada**	Hybrid	Hybrid
Arkansas	Covered		**New Hampshire**	Covered	Covered
California	Covered	Hybrid	**New Jersey**	Hybrid	
Colorado	Other*	Not covered	**New Mexico**	Covered	
Connecticut	Hybrid		**New York**	Hybrid	
Delaware	Hybrid	Hybrid	**North Carolina**	Hybrid	Hybrid
Florida	Hybrid	Hybrid	**North Dakota**	Hybrid	Hybrid
Georgia	Covered	Hybrid	**Ohio**	Hybrid	Hybrid
Hawaii	Hybrid		**Oklahoma**	Covered	Hybrid
Idaho	Hybrid	Hybrid	**Oregon**	Covered	Hybrid
Illinois	Hybrid	Hybrid	**Pennsylvania**	Hybrid	Hybrid
Indiana	Hybrid		**Rhode Island**	Hybrid	
Iowa	Other*		**South Carolina**	Hybrid	Hybrid
Kansas	Hybrid		**South Dakota**	Hybrid	
Kentucky	Hybrid	Hybrid	**Tennessee**	Covered	Covered
Louisiana	Covered	Other**	**Texas**	Hybrid	Hybrid
Maine	Other*	Hybrid	**Utah**	Hybrid	Hybrid
Maryland	Hybrid		**Vermont**	Hybrid	Covered
Massachusetts	Hybrid	Hybrid	**Virginia**	Hybrid	Hybrid
Michigan	Hybrid	Hybrid	**Washington**	Hybrid	
Minnesota	Other*	Not covered	**Wisconsin**	Hybrid	Other***
Mississippi	Covered		**West Virginia**	Hybrid	Hybrid
Missouri	Hybrid		**Wyoming**	Covered	

Hybrid – Hybrid entity
Covered – Single HIPAA covered entity
Not Covered – Not covered by HIPAA
Other* - Neither a hybrid entity nor a covered entity.
Other -** Louisiana's Office of Public Health is part of the state's Department of Health, which is a covered entity in its entirety (including the Office of Public Health).
Other* -** Wisconsin's health department is a non-covered component within Wisconsin Department of Health Services, which is a hybrid entity.

Becoming a Hybrid Entity is Key to Data Sharing

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.[13]

To ensure that PHI is properly protected, HIPAA prohibits the use or sharing of PHI, unless the HIPAA Privacy Rule allows or requires it. The individual who is the subject of the information may also authorize the use or sharing.[14]

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. In fact, HIPAA specifically permits covered entities to share PHI with public health for the purpose of "preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect."[15]

Becoming a hybrid entity is a policy option that carves out non-covered traditional public health components, such as registries, surveillance programs and inspection programs from HIPAA, so that important data sharing can still occur. Applying HIPAA disclosure restrictions to non-covered traditional public health components is typically entirely avoidable and within the control of the health department.

Becoming a hybrid entity limits HIPAA's application, permitting state or local law to continue to govern public health data disclosure. Where public health does not take advantage of this flexibility, it may constrain important data sharing and threaten its mission.

Epidemiological research has improved our health and wellness in countless ways, but is now stunted:

> Notable successes include control of many infectious diseases, identification of numerous carcinogens and other hazardous substances, and improved understanding of modifiable risk factors for many types of diseases, including leading causes of death in the United States such as cardiovascular and respiratory diseases. These advances have led to more effective disease prevention, decreases in disease-related disabilities, and remarkable increases in life expectancy. **Unfortunately, however, the rapidly accelerating movement to limit data access already has impeded or precluded the conduct of many similarly designed studies**.[16]

Access to public health surveillance data, including nationwide birth and death records and disease-specific registries, is increasingly restricted.[17] Routinely collected public health data, including disease surveillance data, vital statistics, intervention data and cause specific mortality data are the most widely collected and most underused data sources.[18] Data custodians often cite HIPAA as the reason for not continuing to make detailed date and location data available. Some estimate the impact of the lack of available data on the public's health to be "substantial."[19]

Public health should explicitly consider these lost opportunities to improve population health and balance them against privacy risks.[20] Applying HIPAA to public health surveillance data is not required by federal law and is not proven to be a superior approach to protecting privacy of this data. Choosing to become a hybrid entity opens the door for public health to evaluate all of its options for protecting privacy, and for releasing more relevant, granular and timely data. Health departments might re-evaluate their HIPAA coverage and become a hybrid entity, if possible.

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

HHS' Office of Civil Rights (OCR) enforces the HIPAA Privacy and Security Rules' compliance requirements against covered entities and business associates.[21] Becoming a hybrid entity may reduce HIPAA compliance burden, risk and exposure. By simple numbers, the fewer components covered by HIPAA, the smaller the HIPAA regulatory footprint.

HIPAA requires workforce training on all policies and procedures.[22] Unless a health department has become a hybrid entity, it is required to train members of the workforce, who never see or touch PHI, on HIPAA privacy and security measures.[23]

HIPAA also requires that complicated assessments and analyses be performed, and that numerous policies and procedures be written and implemented. The combined text of all HIPAA rules is over 100 pages.[24] Beyond the rules, there are FAQs, guidance, commentary and other analyses which exceed the length of the rules by over ten times.[25] Becoming a hybrid entity generally confines application of these complicated and lengthy requirements to only those components where legally required.

When there is a breach of PHI, HIPAA requires notification of affected individuals, HHS and possibly the media.[26] 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. Unless one of three exclusions applies, a covered entity must perform a four-factor risk assessment to determine if the violation rises to the level of a breach.[27] A review of OCR's breach portal, otherwise known as the "Wall of Shame," reflects that in the past twenty-four months, 408 breaches have been reported to OCR. Each breach affects 500 or more individuals, and all are under investigation.[28] By becoming a hybrid entity, a health department removes its traditional public health components from HIPAA's breach notification requirements.[29]

Finally, becoming a hybrid entity may reduce the number of staff who can make mistakes that cause liability under HIPAA.[30]

Begin with an Assessment

To become a hybrid entity, a health department must perform an assessment to determine which organizational components are covered by HIPAA. 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 health department sits.[31] 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 cannot be further legally subdivided. It 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. The health clinic is not separately incorporated. Both the manufacturing firm and the health clinic are part of the same corporation, which is the legal entity.[32] A multi-national corporation with separate subsidiary corporations is not an example of a single legal entity. Each separate corporation is a single legal entity.[33]

Determining the legal entity that "owns" a health department requires more research. Health departments reside within different levels of government and are not private corporations. Not all health departments look alike; there are a variety of operational and legal structures. Generally, there is no governmental filing, akin to a corporation's articles of incorporation, that clearly and legally distinguishes a health department from another government agency. Collaboration between public health practitioners and public health attorneys is key to determining the legal entity.

For purposes of this discussion, the Public Health Accreditation Board's health department classification schema is helpful. Determining the appropriate classification points to next steps for researching the question of the legal entity.

State Health Departments. A state health department is "the governing entity with primary statutory authority to promote and protect the public's health and prevent disease in humans."[34] Fifty-eight percent of state health departments are freestanding or independent. In forty-two percent of states, the health department is a unit within a larger umbrella organization that contains such other functions as Medicaid, mental health, public assistance and substance abuse.[35]

To identify legal authority, begin by reviewing the state's constitution, statutes, regulations or Executive Order. Determine whether the state health department is an independent legal entity or is part of another larger organizational unit, which is the legal entity. If the law is unclear, review Attorney General opinions, which interpret state law; if no opinion exists, evaluate requesting an opinion.[36]

Centralized State Health Departments. A centralized state health department is "a state public health organizational structure that operates all or most of the local health departments."[37] In this model, local health departments are organizational units of the state health department. Review of the legal resources, above, for state health departments should be helpful.

However, even within this structure, larger cities or counties may operate independent local health departments. Review of the legal resources for local health departments, below, will also be necessary.

Local Health Department. 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."[38]

Local health departments may be locally governed; or, a local entity of a centralized state health department; or, a city, city-county, county, district, or regional health department.[39] To determine the legal entity, review the legal resources identified above for state health departments. Also review the charter that defines the organization, responsibilities and authority.[40] The charter functions as a "constitution" for the city or county.[41] Identify and review all city and county codes that pertain to the establishment of the health department. City and county codes are codified ordinances.[42]

Additionally, by charter or ordinance, some local governments give their health departments independence. An independent local health department is the single legal entity. Larger municipalities may provide summaries and guidance regarding key laws and codes, which are instructive.[43]

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

1. Does your health department have authority to sue or be sued in its own name?
2. Is control and supervision of the health department vested within the health 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 the health department? [44]
4. What do relevant organizational charts and websites reflect?

If the health department is not part of a broader organization and is an independent legal entity, the HIPAA assessment should be performed across the health department. If, on the other hand, the health department is part of 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 health department as the legal entity. It is equally applicable to the situation where the health department is part of a larger organization, which is the legal entity.

HIPAA Assessment

A health department is generally a complex organization with a variety of organizational units. Assessing each component against HIPAA is the next step. [45] This assessment involves the identification of components that are covered entities. Covered entities include health plans, health care clearinghouses or health care providers, that engage in one or more standard electronic transactions. The assessment also includes identification of business associates. Most health departments likely have a mixture of covered entities, business associates and non-covered components.

The following examples offer context to HIPAA terminology with respect to a health department.

HIPAA Covered Health Care Provider. A health department's clinic that provides health services to low income individuals and bills health plans electronically for those services, is covered by HIPAA. Even if a health department offers health services, such as vaccinations or sexually transmitted disease screening, in furtherance of health goals, it may be covered by HIPAA. These health services are HIPAA covered if the clinic

bills electronically or utilizes any of the standard electronic transactions in the administrative or financial aspects of health care delivery.[46]

HIPAA Covered Health Plan. If a health department operates a health plan, such as Medicaid or the Children's Health Insurance Program, the relevant components are covered by HIPAA.[47] The assessment should explore all applicable exclusions to ensure coverage is required.[48]

HIPAA Covered Health Care Clearinghouse. It is unlikely that a health department operates a health care clearinghouse. However, if the health department's work involves translating any of the electronic transactions, so that they include standard data elements or vice versus, the health department is operating a health care clearinghouse and that component is covered by HIPAA.[49]

Business Associate. If a health department is covered by HIPAA, it is highly likely that there are internal components providing support services to internal health care providers or health plans that involve sharing PHI. Examples of business associates include public health attorneys, accountants and management.

Public Health Exception to HIPAA. The assessment may identify a number of components that are not covered by HIPAA. The HIPAA Privacy Rule expressly permits covered entities to share PHI, without the patient's authorization, with public health "for the purpose of preventing or controlling disease, injury or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, . . . investigations, and . . . interventions. . ." [50] There are additional public health exceptions listed within this section of the regulation.[51] Additionally, PHI may also be shared with health departments without patient authorization where such disclosure is required by law.[52] This issue brief refers to these non-covered services as traditional public health services.

An example of the public health exception is a state cancer registry where health care providers are required to report cancer cases by name to public health.[53] State law, and not HIPAA, protects the health information received by the health department.[54] A component that provides traditional public health services is not covered by HIPAA.

Hybrid Designation Decision. If the assessment reflects that the health department has any type of covered entity component, the health department is fully covered by HIPAA, by default. This means that HHS could hold the entire health department subject to the HIPAA standards, including components that fall within the exceptions, such as traditional public health components. Where the health department has chosen the hybrid designation, it is important for the health department to take steps to become a hybrid entity. Becoming a hybrid entity generally constrains HIPAA to only those components covered by HIPAA.

An example of a health department that has chosen to become a hybrid entity is where the health department identifies its clinic as a health care provider that bills electronically for services, which is a covered entity under HIPAA. Other components conducting disease reporting and public health surveillance are non-covered.[55] 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.[56]

Responsibilities of the Legal Entity

The legal entity that has chosen to become a hybrid entity has oversight and compliance obligations under HIPAA.

Adoption of Hybrid Entity Policy

To officially become a hybrid entity, the legal entity must have a policy that identifies its components covered by HIPAA; this includes all covered entity and business associate components.[57] Using the example directly above, the health department's hybrid entity policy lists the clinic as its covered entity component.

Legal entities have the option of including health care providers that do not bill electronically—in the hybrid entity policy.[58] 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.[59] Health departments should carefully evaluate this potential advantage against increased regulatory burden, risk and liability.

Legal entities must memorialize the hybrid entity in writing or record it electronically; without this "formality," the health department is not actually a hybrid entity and is fully covered by HIPAA.[60] 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.

Review 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. Research reveals that some organizations require annual HIPAA assessment, thus identifying the need for updating the hybrid entity policy in a timely manner.

Compliance with HIPAA Privacy and Security Rules

The legal entity must ensure that covered entity and business associate components do not use or disclose PHI in violation of HIPAA.[61] Particular attention must be paid to confirm that sharing between the covered components and non-covered components does not violate HIPAA. Additionally, the legal entity must verify that appropriate HIPAA privacy and security policies and procedures are adopted.

Finally, the legal entity is responsible for making certain that all related contracts, including business associate agreements and other organizational requirements, are in place.[62] Federal guidance suggests that the legal entity enter into contracts and conduct other organizational matters at its level, instead of at a lower level.[63]

HIPAA Re-Assessment is Important

Changes in law and heightened HIPAA enforcement activity make re-assessing HIPAA coverage a priority. This should also be a priority for health departments that have already become a hybrid entity.

Omnibus Rule Changes

There have been two changes in law that impact becoming a hybrid entity since many organizations created or updated their hybrid entity policies.

In 2013, OCR promulgated the Final Omnibus Rule which changes the requirements for becoming a hybrid entity. Strengthening HIPAA's privacy and security protections, this rule implements provisions of the Health

Information Technology for Economic and Clinical Health or HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009. Previously, the legal entity had discretion as to whether to include components that function as business associates.[64] Today, regulation requires that the hybrid entity policy include both covered entity and business associate components.[65] OCR continues to allow legal entities discretion as to whether to include health care providers that do not bill electronically in the hybrid entity policy.[66]

Additionally, OCR greatly expanded the definition of business associate, including many new types of organizations: health information organizations, e-prescribing gateways, record locator services, data/records storage or cloud computing services, and personal health record vendors.[67] Business associates now include subcontractors and their subcontractors' subcontractors.[68] Only internal subcontractors are listed in the hybrid entity policy.

Health departments should review their hybrid entity policies to make certain that all business associate components are included.

Office of Civil Rights Enforcement Action

Failure to include each covered entity and business associate component in the hybrid entity policy is a HIPAA violation and may result in regulatory enforcement action by OCR.[69] As of December 2018, OCR has settled or imposed a civil monetary penalty in 62 cases, totaling $96,581,582.00.[70] Additionally, OCR settled a potential HIPAA violation with a county government that operates a local health department. [71]

In 2016, OCR agreed to a settlement with the University of Massachusetts Amherst (UMass) for potential HIPAA violations that included failure to correctly identify all HIPAA covered entity components in its hybrid entity policy. [72] Three years earlier, UMass reported to OCR that it had a workstation that was infected with malware causing a breach of PHI of 1,670 patients – names, addresses, Social Security numbers, dates of birth, health insurance information, diagnoses and procedure codes. This workstation was located in UMass' Center for Language, Speech, and Hearing. UMass had not identified the Center as a covered entity component in its hybrid entity policy and it was not HIPAA compliant. Additionally, UMass did not have a firewall in place, which allowed the malware to gain access to its system.

To settle these alleged violations, UMass agreed to a corrective action plan and to make a monetary payment of $650,000.[73] This settlement agreement underscores the significance of an accurate hybrid entity policy that identifies all of the required components. When components are omitted from the hybrid entity policy, and the resulting compliance effort, HIPAA's privacy and security safeguards are likely not in place to protect the PHI.[74]

This case demonstrates that it is challenging to analyze HIPAA coverage and that there are not always "bright lines" distinguishing when a component is covered by HIPAA and when it is not.[75] Additionally, organizations may change structure and function over time. If your health department has not completed a HIPAA assessment within the past year, it should do so to identify any needed changes in its hybrid entity policy.

Conclusion

HIPAA re-assessment is a priority. HIPAA constrains data sharing and its coverage should be re-examined. Changes in law, technology, function, organization and process also drive the need for re-assessment. Identifying where HIPAA requires compliance in health departments and adopting a hybrid entity policy to

formalize this option might position public health to appropriately share more data, achieve improved HIPAA compliance and reduce risk.

SUPPORTERS

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

This document was prepared by Denise Chrysler, JD, Director, with the Network for Public Health Law – Mid-States Region at the University of Michigan School of Public Health, and Sallie Milam, JD, 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] 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] 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 codes and identifying numbers used in these transactions be standardized. HHS. (2017, June 16). *HIPAA Home: HIPAA for Professionals*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/index.html.

[3] References to being "covered by HIPAA" also mean "covered function," "covered entity" and "business associate."

[4] Definitions and examples of each type of covered entity is provided in the next section.

[5] CMS Transactions, *supra* note 3.

[6] 45 CFR § 160.103.

[7] IOM 4, *supra* note 1.

[8] 45 CFR § 160.103.

[9] *Id*.

[10] 45 CFR § 164.103.

[11] *Id*.

[12] Association of State and Territorial Health Officials. (2005). *HIPAA Privacy Rule Implementation in State Public Health Agencies — Successes, Challenges, and Future Needs.* Retrieved from https://biotech.law.lsu.edu/cdc/astho/HIPAA5FINAL.pdf.

[13] 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

[14] *Id*.

[15] *Id*.

[16] Wartenberg, D., & Thompson, W. D. (2010). Privacy Versus Public Health: The Impact of Current Confidentiality Rules. American Journal of Public Health, 100(3), 407–412. (Citations omitted, emphasis added). http://doi.org/10.2105/AJPH.2009.166249. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2820076/, p. 2.

[17] *Id*. at 3.

[18] Van Panhuis, W. G., Paul, P., Emerson, C., Grefenstette, J., Wilder, R., Herbst, A. J., … Burke, D. S. (2014). A systematic review of barriers to data sharing in public health. *BMC Public Health*, *14*, 1144. http://doi.org/10.1186/1471-2458-14-1144. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4239377/#CR2 at p. 3.

[19] Wartenberg, *supra* note 18.

[20] Van Panhuis, *supra* note 20.

[21] 45 CFR Part 160, Subparts C, D and E.

[22] 45 CFR § 164.530.

[23] *See*, Bakewell, C.M. (2012). Municipalities as Hybrid Entities under HIPAA. *The Missouri Municipal Review*, 24. Retrieved from http://c.ymcdn.com/sites/www.mocities.com/resource/resmgr/september_2012_review/munichybridentitiesunderhipa.pdf?hhSearchTerms=%22hipaa%22.

[24] 45 CFR Parts 160, 162, and 164.

[25] HHS. (2016, June 16). *HIPAA for Professionals*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/index.html.

[26] 45 CFR § 164.400 *et seq*.

[27] *Id*.; *see* Bakewell, *supra* note 25.

[28] Office of Civil Rights. *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. Retrieved January 2018 from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[29] Bakewell, *supra* note 25.

[30] Fellows, M. (2003). THE HIPAA "PRIVACY RULE." *League of California Cities*. Retrieved from https://www.cacities.org/uploadedfiles/leagueinternet/b1/b1e39976-4976-414c-96c6-ed57a04623ac.pdf.

[31] 45 CFR § 164.103.

[32] 65 FR 82462, 82502, Preamble from December 28, 2000.

[33] *Id*.

[34] Public Health Accreditation Board. *Who is eligible?* Retrieved from http://www.phaboard.org/accreditation-overview/who-is-eligible/.

[35] Association of State and Territorial Health Officials. (2017, November). ASTHO Profile of State & Territorial Public Health, vol. 4. Retrieved from http://www.astho.org/Profile/Volume-Four/2016-ASTHO-Profile-of-State-and-Territorial-Public-Health/; *see also*, Public Health Law Center at William Mitchell College of Law. (2015, April). *State & Local Public Health: An Overview of Regulatory Authority*. Retrieved from http://www.publichealthlawcenter.org/sites/default/files/resources/phlc-fs-state-local-reg-authority-publichealth-2015_0.pdf.

[36] *See*, Social Security Administration. *State and Local Government Employers – Information: How To Determine An Entity's Legal Status*. Retrieved from https://www.ssa.gov/section218training/advanced_course_9.htm.

[37] PHAB, *supra* note 36.

[38] *Id*.

[39] *Id*.

[40] *See*, Internal Revenue Service. (2017, August 17). *Government Entities and Their Federal Tax Obligations: What are Government Entities and Their Federal Tax Obligations?* Retrieved from https://www.irs.gov/government-entities/federal-state-local-governments/government-entities-and-their-federal-tax-obligations.

[41] Egler, P. (2001). What Gives Cities and Counties the Authority to Create Charters, Ordinances, and Codes? *Perspectives Teaching Legal Research and Writing*, 9, 145. Retrieved from https://info.legalsolutions.thomsonreuters.com/pdf/perspec/2001-spring/spring-2001-10.pdf.

[42] *Id*. at 146.

[43] *See*, City of Boston. Statutes and Ordinances Governing Boston's Operating and Capital Budgets 16(1), 222. Retrieved from https://www.boston.gov/sites/default/files/fy16-volume1-statutes-ordinances.pdf; City of Boston. Guide to the Public Health Commission Boards records. Retrieved from https://www.cityofboston.gov/images_documents/Guide%20to%20the%20Public%20Health%20Commission%20records_tcm3-20744.pdf.

[44] *See*, IRS, *supra* note 42.

[45] HHS. (2002, December 20). *FAQ: Are state, county or local health departments required to comply with the HIPAA Privacy Rule?* Retrieved from https://www.hhs.gov/hipaa/for-professionals/faq/358/are-state-county-or-local-health-departments-required-to-comply-with-hipaa/index.html.

[46] Centers for Disease Control and Prevention. (2003, April 11). *MMWR: HIPAA Privacy Rule and Public Health, Guidance from CDC and the U.S. Department of Health and Human Services*. (CDC Guidance). Retrieved from https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm at pp. 10 – 11.

[47] *Id*. at 11.

[48] 45 CFR § 160.103.

[49] *Id*.

[50] 45 CFR § 164.512(b); CDC Guidance, *supra* note 48.

[51] *Id*.

[52] 45 CFR § 164.512(a); CDC Guidance, *supra* note 48. Later amendments to HIPAA, known as the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Omnibus Rule, continue the public health purpose exception. Goldstein, M. M., & Pewen, W. F. (2013). The HIPAA Omnibus Rule: Implications for Public Health Policy and Practice. *Public Health Reports*, *128*(6), 554–558. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3804103/.

[53] CDC Guidance, *supra* note 48.

[54] Kamoie, B. and Hodge, J. (2004). Law and the Public's Health; HIPAA's Implications for Public Health Policy and Practice: Guidance from the CDC. *Public Health Reports*, 119, 216. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1497612/pdf/15192909.pdf.

[55] *Id*. at 218.

[56] Broome, C., Horton, H., Tress, D., Lucido, S. & Koo, D. (2003). Statutory Basis for Public Health Reporting Beyond Specific Diseases. Journal of Urban Health: Bulletin of the New York Academy of Medicine, 80 (2, Supp. 1), i14, i17. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3456544/pdf/11524_2006_Article_190.pdf; Association of State and Territorial Health Offices. (2004). Information Management for State Health Officials: Data Sharing with Covered Entities under the HIPAA Privacy Rule, A Review of Three State Public Health Approaches. Retrieved from https://biotech.law.lsu.edu/cdc/astho/29408_ASTHO.pdf at p. 7.

[57] This is also known as designation of health care components. 45 CFR § 164.103.

[58] 45 CFR § 164.105(a)(2)(iii)(D).

[59] 45 CFR § 164.506(c)(4).

[60] 45 CFR § 164.103.

[61] 45 CFR § 164.105(a)(2)(ii).

[62] 45 CFR § 164.105(a)(2)(iii).

[63] 78 FR 5566, 5589, Preamble.

[64] Former 45 CFR § 164.504(c)(3)(iii).

[65] 45 CFR § 164.105(a)(2)(iii); Bernstein, J. (2013). Implications for Covered Entity Public Health Agencies under the HIPAA Omnibus Rule. *ABA HEALTH eSOURCE*, 9(9), 2. Retrieved from https://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/aba_health_law_esource_1305_bernstein.html.

[66] 45 CFR § 164.105(a)(2)(iii)(D).

[67] 45 CFR § 160.103; Health Information & the Law. (2013). *Fast Facts: Are You a Business Associate Under the HIPAA Privacy and Security Rules?* Retrieved from http://www.healthinfolaw.org/article/fast-facts-are-you-business-associate-under-hipaa-privacy-and-security-rules.

[68] *Id*.

[69] 45 CFR § 164.105(a)(2)(iii).

[70] HHS. (2019, January 29). *Health Information Privacy: Enforcement Highlights*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[71] HHS. (2017, June 7). *Examples: County Government Settles Potential HIPAA Violations*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/skagit-county/index.html.

[72] HHS. (2016, November 20). *Agreements: UMass settles potential HIPAA violations following malware infection – November 22, 2016*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/umass.

[73] *Id*.

[74] Baker Donelson. (2016, November 30). *Publications: OCR Examines Hybrid Entity Designation in Latest HIPAA Settlement*. Retrieved from https://www.bakerdonelson.com/ocr-examines-hybrid-entity-designation-in-latest-hipaa-settlement.

[75] HITECH Answers. (2016, December 19). *Mixing It Up: HIPAA Hybrid Entities*. Retrieved from https://www.hitechanswers.net/mixing-hipaa-hybrid-entities/.