

How Does the HIPAA Privacy Rule Apply to Health Plans in NC Local Government?

Aimee Wall
UNC School of Government

I. What is HIPAA? What is the privacy rule?

- A. **HIPAA:** The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the U.S. Department of Health and Human Services (U.S. DHHS) to develop a series of rules governing health information. In general, the rules are intended to standardize the communication of electronic health information between health care providers and health insurers. In addition, the rules are intended to protect the privacy and security of individually identifiable health information. Several of the HIPAA rules have been published in final form, including the privacy and security rules.
- B. **The HIPAA Privacy Rule** (Code of Federal Regulations, Title 45, Part 164): The HIPAA privacy rule governs how “covered entities” may use and disclose “protected health information.” This outline reviews the definition of “covered entity” as it applies to health plans in local government. The detailed requirements of the privacy rule are summarized in other outlines and materials available from the Institute of Government. See www.medicalprivacy.unc.edu. Covered entities (with the exception of small health plans) must be in compliance with the Privacy Rule by April 14, 2003. Small health plans must be in compliance by April 14, 2004.

II. Who is regulated by the HIPAA privacy rule?

- A. **“Covered entities” are regulated:** HIPAA directly regulates the following three types of “covered entities”:
 - 1. Health plans;
 - 2. Health care clearinghouses (entities that help health care providers and health plans standardize their health information); and
 - 3. Health care providers who transmit health information in electronic form in connection with a HIPAA transaction.

B. HIPAA Definitions – Health Plans

1. The term “health plan” is defined in HIPAA to mean an individual or group plan that provides, or pays the cost of, medical care. 45 C.F.R. § 160.103. The term includes (but is not limited to):
 - a. A group health plan (see discussion below);
 - b. A health insurance issuer (an insurance company, insurance service, or insurance organization (including an HMO but not a group health plan) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance);
 - c. An HMO;
 - d. The Medicare program;
 - e. The Medicaid program;
 - f. A Children’s Health Insurance Program (CHIP) plan (“Health Choice” in North Carolina);
 - g. An issuer of a Medicare supplemental policy (a “Medigap” policy);
 - h. An issuer of a long-term care policy (excluding a nursing home fixed-indemnity policy);
 - i. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers;
 - j. Military and veterans’ health care programs;
 - k. The Indian Health Service;
 - l. The Federal Employees’ Health Benefits Program;
 - m. A high-risk pool (North Carolina does not currently have one); and
 - n. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in 42 U.S.C. 300gg-91(a)(2)).

2. The term “health plan” does not include:
 - a. Any policy, plan, or program to the extent that it provides, or pays for the cost of excepted benefits (including, for example, accident/disability income insurance, liability insurance, and workers’ compensation) (See 42 U.S.C. 300gg-91(c)(1));
 - b. A government-funded program whose principal purpose is other than providing, or paying the cost of, health care;
 - c. A government-funded program whose principal activity is the direct provision of health care to persons; and
 - d. A government-funded program whose principal activity is the making of grants to fund the direct provision of health care to persons.

3. Group health plan: The term “group health plan” is a subset of the term “health plan.” The definition of the term relies heavily on terms used in the Employee Retirement Income Security Act of 1974 (ERISA), but it is important to note that some plans that are not subject to ERISA are still considered group health plans under HIPAA (specifically “governmental plans”). All group health plans are covered entities.
 - a. The term “group health plan” includes *employee welfare benefits plans* (as that term is defined in ERISA; see below), including insured and self-insured plans, to the extent that the plan provides medical care (including items and services paid for as medical care) to employees or their dependents directly or through insurance, reimbursement, or otherwise, that has 50 or more participants or is administered by an entity other than the employer that established and maintains the plan. A “group health plan” is a separate legal entity from the employer but it generally does not have its own employees or operations. The operations of a group health plan are often shared between other entities, which may include the employer (plan sponsor), a health insurance company or HMO, and/or a third-party administrator.
 - b. The term “employee welfare benefit plan” is defined in ERISA to mean “any plan, fund, or program ... established or maintained by an employer or by an employee organization, or by both, to the extent that such plan, fund, or program was established or is maintained for the purpose of providing for its participants or their beneficiaries, through the purchase of insurance or otherwise, (A) medical, surgical, or hospital care or benefits....” 29 U.S.C. 1002.
 - c. Many health plans offered by local government employers are not subject to ERISA but they are still included within the definition of the term “employee welfare benefit plan” and therefore may be “group health plans” subject to HIPAA.¹
4. Plan sponsor: The Privacy Rule adopts the definition of “plan sponsor” used in ERISA. 45 C.F.R. § 164.103 (Privacy Rule); 29 U.S.C. 1002(16)(B) (ERISA). ERISA defines the term to mean:
 - a. The employer in the case of an employee benefit plan established or maintained by a single employer;
 - b. The employee organization in the case of a plan established or maintained by an employee organization; or

¹ The plans offered by government employers meet the definition of “employee welfare benefit plan” in ERISA, but the *employers* are exempt from ERISA under 29 USC 1003(b)(1).

- c. In the case of a plan established or maintained by two or more employers or jointly by one or more employers and one or more employee organizations, the association, committee, joint board of trustees, or other similar group of representatives of the parties who establish or maintain the plan.
5. Small health plan: “Small health plans” have an additional year to come into compliance with the privacy rule. A small health plan is defined as a health plan with annual receipts of \$5 million or less. 45 CFR § 160.103.² DHHS recently explained the two different means for calculating annual receipts:
- a. Health plans that report receipts to the IRS: Health plans that file certain federal tax returns and report receipts on those returns should use the following guidance provided by the Small Business Administration at 13 C.F.R. § 121.104 to calculate annual receipts:
 - i. “Receipts” means “total income” (or in the case of a sole proprietorship, “gross income”) plus “cost of goods sold” as these terms are defined or reported on Internal Revenue Service (IRS) Federal tax return forms; Form 1120 for corporations; Form 1120S for Subchapter S corporations; Form 1065 for partnerships; and Form 1040, Schedule F for farm or Schedule C for sole proprietorships). However, the term “receipts” excludes net capital gains or losses, taxes collected for and remitted to a taxing authority if included in gross or total income, proceeds from the transactions between a concern and its domestic or foreign affiliates (if also excluded from gross or total income on a consolidated return filed with the IRS), and amounts collected for another by a travel agent, real estate agent, advertising agent, conference management service provider, freight forwarder or customs broker. In calculating receipts under this guidance, health plans should use the definitions and process described at 13 C.F.R. § 121.104(a)(2) - (3) and § 121.104(b).
 - b. Health plans that do not report receipts to the IRS: Health plans that do not report receipts to the IRS (including, for example, group health plans that are exempt from filing income tax returns) should use proxy measures to determine their annual receipts.
 - i. Fully-insured health plans should use the amount of total premiums which they paid for health insurance benefits during the plan’s last full fiscal year.

² See the “Frequently Asked Questions” section of www.cms.hhs.gov/hipaa/hipaa2/default.asp for more information from DHHS regarding the definition of small health plan.

- ii. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer, plan sponsor or benefit fund, as applicable to their circumstances, on behalf of the plan during the plan's last full fiscal year. Those plans that provide health benefits through a mix of purchased insurance and self-insurance should combine the proxy measures to determine their total annual receipts.

C. "Health plans" in NC local government

1. Group health plans: Overview of the different models of group health plans
 - a. Fully-insured: Many employers pay a premium to a health insurance company in order to extend health insurance coverage to employees. In this model, the insurance company reimburses health care providers and employees directly for medical expenses. The insurance company, rather than the employer, is bearing the risk for medical expenses incurred by one or more of the plan participants (i.e., employees and their dependents).
 - i. Plan sponsor: The employer is the plan sponsor. It is not a covered entity.
 - ii. Group health plan: The actual "health plan" under ERISA and HIPAA is a separate legal entity from the employer (and is generally a legal entity that largely exists only on paper). The health plan is a covered entity.
 - iii. Insurance company or HMO: The employer is paying a premium to an insurance company or HMO. That insurance company or HMO is also a covered entity under HIPAA and must comply with the Privacy Rule with respect to its own operations.

- b. Self-insured: Some employers have established “self-insured” health plans. In this model, the employer pays for some of the medical costs incurred by enrolled employees and their dependents.³ The employer may contract with a “third party administrator” to process claims from providers and participants, communicating with employees, and fulfilling other administrative duties.
 - i. Plan sponsor: The employer is the plan sponsor. It is not a covered entity.
 - ii. Group health plan: The actual “health plan” under HIPAA is a separate legal entity from the employer (and is generally a legal entity that exists only on paper). The health plan is a covered entity. In practice, the employer/plan sponsor’s employees often serve in some capacity as administrative representatives of self-insured health plans.
 - iii. Third-party administrator: The employer generally contracts with an organization (that may or may not be a covered entity) to act as the third-party administrator (TPA) for the health plan. The TPA would be considered a “business associate”⁴ of the covered entity (the group health plan).

2. Other health plans to consider

- a. Health care spending accounts (Flexible Spending Accounts): Recall that the definition of “health plan” includes a catch-all provision for “any other individual or group plan ... that provides or pays for the cost of medical care.” Spending accounts, depending on how they are organized, may fall within this catch-all definition. The term “medical care” referred to in this catch-all means amounts paid for “the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any structure or function of the body” including:
 - i. Transportation primarily for and essential to such medical care; and
 - ii. Insurance covering such medical care and transportation.

³ Employers may also arrange for stop-loss or reinsurance coverage to prevent the employer from incurring costs over a certain threshold.

⁴ A “business associate” is a person or an entity (other than a member of the covered entity’s workforce) that uses PHI to either perform functions or activities *on behalf of* a covered entity (such as claims processing or quality assurance) or provide one of several specific services (including legal, accounting, and accreditation services). See 45 C.F.R. § 160.103. The privacy rule imposes several requirements on business associate relationships. For example, in most circumstances, the covered entity and the business associate must enter into a written contract that requires the business associate to take specific steps to protect PHI. See 45 C.F.R. §§ 164.502(e); 164.504(e).

- b. Employee assistance programs (EAPs): Many employers offer employee assistance programs, which vary widely with respect to services, funding and organization. These programs may fall within the catch-all “health plan” definition.⁵

III. General rules governing group health plans

A. Limitations on group health plans disclosing PHI to the plan sponsor

1. De-identified information: A group health plan (or an insurance company or HMO working with a plan) will always be allowed to disclose “de-identified” information to a plan sponsor. 45 C.F.R. §§ 164.502(d); 164.514(a)-(c). Information that has been appropriately de-identified is not considered “PHI” under the Privacy Rule and therefore is not subject to the Rule’s complex restrictions on use and disclosure. The Rule outlines two methods for de-identifying information:
 - a. Information may be considered de-identified if all unique identifying numbers, characteristics or codes have been removed, including 17 specific identifiers (including name, address, social security number, medical record number). In addition, if this method of de-identification is chosen, the health plan disclosing the information must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual.
 - b. Information may be considered de-identified if a statistical expert determines that the “risk is very small that the information could be use, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual.” The covered entity must document the expert’s methods and analysis.

⁵ These programs meet the definition of “health care provider” under HIPAA as well. Note that a health care provider will *only* be a covered entity under HIPAA if the provider also transmits health information electronically in connection with a HIPAA transaction (such as electronically transmitting a bill for health care services to an insurance company). See 45 C.F.R. §160.103 (definitions of covered entity and health care provider).

2. Summary health information: A group health plan may disclose summary health information to a plan sponsor in limited circumstances. 45 C.F.R. § 164.504(a) & (f).
 - a. What is summary health information? The term “summary health information” is defined to include information that:
 - i. Summarizes the claims history, claims expenses or types of claims experienced by individuals in the group health plan; and
 - ii. As with the second type of de-identified information described above, does not include any unique identifying numbers, characteristics or codes. Unlike de-identified information, however, summary health information may include certain geographic identifiers (i.e., zip codes).
 - b. When may it be disclosed to plan sponsor? SHI may be disclosed to the plan sponsor without the individual’s permission if the plan sponsor requests the information for the purpose of either:
 - i. Obtaining premium bids from health plans for providing health insurance coverage under the plan; or
 - ii. Modifying, amending, or terminating the group health plan.
3. Enrollment/disenrollment information: A group health plan may disclose information to the plan sponsor on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan to the plan sponsor without the individual’s permission. 45 C.F.R. § 164.504(f)(1)(iii).
4. Authorization: A group health plan may disclose any PHI to a plan sponsor pursuant to the individual’s written authorization. The Privacy Rule includes detailed requirements regarding the content of authorization forms and the rules governing the use of such forms. 45 C.F.R. § 164.508.
5. Plan document amendments: If the disclosure does not fall within one of the four categories described above, the group health plan may only disclose PHI to a plan sponsor only if it amends the plan documents and complies with the other requirements described below. 45 C.F.R. § 164.504(f).
 - a. Amendments: If the plan intends to disclose PHI to the plan sponsor for purposes other than those described above, the plan documents must be amended to:
 - i. Establish the permitted and required uses and disclosure of such information by the plan sponsor. These uses and disclosures must be consistent with the requirements of the privacy rule.

- ii. Provide that the plan will disclose PHI to the plan sponsor only after the plan sponsor certifies that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to comply with the provisions. The required amendments must provide that the plan sponsor will:
 - (1) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;
 - (2) Ensure that any agents receiving PHI from the plan sponsor agree to the same restrictions and conditions that apply to the plan sponsor;
 - (3) Not use or disclose the information for employment-related actions and decisions;
 - (4) Not use or disclose the information in connection with any other benefit or employee benefit plan of the plan sponsor;
 - (5) Report to the group health plan any inappropriate use or disclosure of the information;
 - (6) Make PHI available for inspection, copying, and amendment and make any amendments to PHI as appropriate;
 - (7) Make information available such that an accounting of disclosures may be provided upon request;
 - (8) Make its internal practices, books, and records relating to use and disclosure of PHI available to DHHS for compliance activities;
 - (9) Return or destroy PHI received from the group health plan if feasible (if return or destruction is not feasible, limit further use and disclosure of the PHI to those purposes that make the return or destruction infeasible); and
 - (10) Ensure adequate separation between the group health plan and the plan sponsor by describing the employees under the control of the plan sponsor with access to PHI, restricting such employees' access to and use of PHI to plan administration functions and providing a mechanism for resolving issues of noncompliance by such employees.

- b. Disclosure permitted for plan administration functions: If the documents are amended, the group health plan may disclose PHI to plan sponsor to carry out "plan administration functions" that the plan sponsor performs. "Plan administration functions" are defined as "administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor." 45 C.F.R. §164.504(a).

- c. Disclosure not permitted: Even if the documents are amended, the group health plan (or an insurance company or HMO working with the plan) must not disclose PHI to plan sponsor:
 - i. For the purpose of employment-related actions or decisions; or
 - ii. In connection with any other benefit or employee benefit plan of the plan sponsor.

- d. Notice of privacy practices: The Privacy Rule requires covered entities to develop a notice of privacy practices that, among other things, is a detailed description of how the entity uses and disclose PHI. In order for the group health plan to disclose PHI to the plan sponsor the notice must include a statement explaining that such disclosures will take place. See 45 C.F.R. §§ 164.504(f)(3)(iii); 164.520(b)(1)(iii)(C).

B. Compliance responsibilities for group health plans

1. Fully-insured group health plans

- a. Group health plan receiving “limited PHI”⁶: If a fully-insured group health plan⁷ does not create or receive PHI except for de-identified information, summary health information, enrollment/disenrollment information, and information pursuant to an authorization (see Section III.A.1. through A.5 above), the group health plan would have limited compliance responsibilities under the privacy rule. In this situation, the group health plan would be contracting with an insurance company or an HMO to provide the health insurance and that company/HMO would be a covered entity in its own right and would have its own responsibilities under the privacy rule. These group health plans should still review the Privacy Rule and ensure that they are in compliance with the applicable requirements. For example:
 - i. Notice: Covered entities are required to provide individuals with a written notice of privacy practices. In this situation, both the group health plan and the insurance company/HMO are covered entities and therefore they both have a duty to provide a notice to the enrollees in the plan. Rather than provide enrollees with two notices, the group health plan could enter into an organized health care arrangement (OHCA) (see Section IV below) with the insurance company/HMO which would, among other things, allow the insurance company/HMO to issue a “joint notice” to the enrollees on behalf of both the group health plan and the company/HMO. This would satisfy the group health plan’s obligation to provide a notice to its enrollees.

⁶ The term “limited PHI” plan is borrowed from HIPAA training and assistance materials prepared by Mike Hubbard of Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P. (Raleigh, NC).

⁷

- ii. Administrative requirements: This type of fully-insured group health plan is exempt from most of the administrative requirements in the privacy rule (specified in 45 C.F.R. § 164.530), such as the requirement to draft written policies and procedures. The group health plan must still comply with the following three administrative requirements:
 - (1) The plan must refrain from intimidating or retaliatory acts against persons exercising rights under the privacy rule (e.g., an individual requesting a copy of his or her record or filing a complaint) and against persons opposing practices that the person believes to be contrary to the requirements of the privacy rule.
 - (2) The plan may not require individuals to waive their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
 - (3) If the group health plan amends the plan documents, it must maintain documentation of the amendments for six years from the date of the amendment's creation or the date the amendment was last in effect, whichever is later.
 - iii. Other Privacy Rule requirements: In order to ensure that all of the requirements of the Privacy Rule are satisfied, the group health plan/plan sponsor should communicate and coordinate with the insurance company/HMO providing the insurance to its enrollees.
- b. Plan sponsor not receiving limited PHI: If the plan sponsor is not receiving the limited types of PHI described above, the group health plan will have to amend the plan documents (see Section III.A.5. above) and ensure compliance with all applicable requirements of the privacy rule. It is possible that the health insurance company/HMO will assume responsibility for some of the administrative compliance responsibilities, but the group health plan must recognize that it has independent compliance responsibilities under the Rule. Therefore, it is in the group health plan's interest to coordinate with the insurance company/HMO.
2. Self-insured group health plans: Plan sponsors of self-insured plans (usually human resources departments) generally assume responsibility for more plan administration functions. As a result, these plans typically share more than "limited PHI" with the plan sponsor. Therefore, these self-insured group health plans will have to amend the plan documents (see Section III.A.5 above) and ensure compliance with all applicable requirements of the privacy rule. The group health plan may negotiate a contract with the third-party administrator (TPA) to have the TPA assist with some of the compliance functions.

IV. Organized Health Care Arrangements (OHCA)

- A. What is an “OHCA”? The privacy rule permits certain groups of legally separate covered entities to streamline some compliance efforts if the entities meet the definition of an “organized health care arrangement” (OHCA). 45 C.F.R. § 164.501. There are several types of OHCA, only three of which are relevant for group health plans. An plan-oriented OHCA may consist of:
1. A group health plan and a health insurance company/HMO (but only with respect to PHI created or received by the company/HMO that relates to enrollees of the group health plan);
 2. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
 3. Such same-sponsor group health plans (see above) and health insurance companies/HMOs (but only with respect to PHI created or received by the company/HMO that relates to enrollees of the group health plans).
- B. How does participating in an OHCA streamline compliance efforts?
1. Joint notice: Entities participating in an OHCA may elect to develop and use a joint notice if they comply with all of the requirements described below. 45 C.F.R. § 164.520(d). If the entities were not participating in an OHCA, each entity would be required to provide a notice. In addition to all of the requirements generally applicable to notices of privacy practices, the following special requirements apply to joint notices:
 - a. Notice is binding: The participating entities must agree to abide by the terms of the notice with respect to PHI created or received by the entity as part of its participation in the OHCA.
 - b. Content: The joint notice must include all of the same elements as a standard notice and it must also include additional elements specified in 45 C.F.R. § 164.520(d).
 - c. Dissemination: If one of the entities participating in the OHCA provides an individual with the OHCA’s joint notice, then all of the covered entities participating in the OHCA will be in compliance with the dissemination requirements.

2. Business associates: A covered entity participating in an OHCA that performs business associate functions to or for the OHCA does not become a business associate of the other entities participating in the OHCA with respect to those functions. If the entities were not participating in an OHCA, the entity acting as a business associate of the other entities would be required to comply with all of the business associate requirements (including having a business associate agreement). 45 C.F.R. § 160.103 (definition of business associate).
3. Health care operations: An entity participating in an OHCA may disclose PHI about an individual to another covered entity participating in the OHCA for any health care operations activities of the OHCA. 45 C.F.R. § 164.506(c)(5).⁸ If the entities were not participating in an OHCA, they would only be permitted to disclose PHI to another entity for health care operations activities of the other entity in limited circumstances.

⁸ The term “health care operations” is defined in detail in the privacy rule. See 45 C.F.R. § 164.501. In general, the term encompasses many of the activities that support the treatment and payment activities of providers and health plans such as quality assurance efforts, underwriting, customer service and management activities.