HIPAA AND EMPLOYER GROUP HEALTH PLANS: *NOTHING IS SIMPLE*

Beth L. Rubin
Dechert LLP

Introduction

Health plans, health care providers and clearinghouses have been scrambling to develop programs for complying with the privacy regulations ("Privacy Standards") issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[1] The trade press and listserves have discussed at length how these regulations affect the operations of providers and payors, and recently have begun to address how the regulations affect group health plans. Very little has been published about employer group health plans, however. In fact, while many provider organizations have their HIPAA privacy compliance programs well under way, many are just beginning to focus on how the privacy regulations affect the other covered entity in their midst: their employee group health plan. Many employers outside of the health care industry, moreover, also are just beginning to understand that their health plan may be a covered entity under HIPAA or what this may mean to them.

Employer group health plans must comply with all the same Privacy Standards that apply to providers and clearinghouses, plus certain Standards that apply only to health plans. This outline and presentation will briefly summarize the standards that are common to all covered entities (noting where these common standards apply differently to health plans), and then focus in more detail on the Standards that apply only to health plans. I also will address a number of practice issues relating to employer group health plans.

I. General Privacy Standards

All covered entities, including employer group health plans (defined below), must comply with Privacy Standards relating to the following:

1. 45 C.F.R. Parts 160 and 164.

A. Restrictions on Uses and Disclosures of PHI

1. Covered entities may not use or disclose protected health information ("PHI") except as permitted or required under the Privacy Standards;[2]

2. Treatment, payment, and health care operations ("TPO");[3]

3. Authorizations for uses and disclosures not otherwise permitted by the Privacy Standards;[4]

4. Uses and disclosures requiring an opportunity for the individual to agree or object;[5]

5. Uses and disclosures for which an authorization, or opportunity to agree or object is not required;[6]

6. "Minimum necessary" standard;[7]

7. Business associate requirements;[8] and

8. De-identification standards.[9]

---

2. 45 C.F.R. § 164.502(a).

3. *See* definitions of these terms in 45 C.F.R. § 164.501, and Standards in § 164.506.

4. *See* 45 C.F.R. § 164.508.

5. *See Id*. § 164.510.

6. *See Id*. § 164.512.

7. *See Id*. § 164.502(b).

8. *See Id*. §§ 164.502(e), 164.504(e).

9. *See Id*. § 164.514.

B. Individual (Plan Member) Rights Requirements

1. Right to Notice of Privacy Practices ("NPP").[10]

- Health plans need not obtain "acknowledgment" of receipt of NPP;
- Strict NPP content requirements;
- Plans must provide notice to members by the compliance date and thereafter to new members at the time of enrollment;
- Insured plans that do not receive PHI do not have to provide an NPP to plan members -- the NPP is provided by the insurer or HMO;
- Insured plans that create or receive PHI must maintain a NPP and provide it upon request; and
- The NPP delivery requirement is satisfied if the plan provides the NPP to the named insured -- plans need not provide a NPP to each dependent.

2. Right to Request Restrictions of Uses and Disclosures.[11]

- Plans need not agree to requested restrictions;
- Must provide a confidential mode of communication (by alternative means or at alternative locations) if a plan member states that disclosure of PHI could endanger the individual.

3. Right to Access PHI.[12]

- Plan members have the right to access, inspect, and copy their PHI;
- Strict deadlines and procedures.

---

10. *See Id*. § 164.520.

11. *See Id*. § 164.522.

12. *See Id*. § 164.524.

4. Right to Amend PHI.[13]

- Plans may deny requests for amendment if the PHI was not created by the plan or is accurate and complete;
- Strict deadlines and procedures.

5. Right to an Accounting of Certain Disclosures of PHI.[14]

- Multiple exceptions;
- Strict deadlines, content requirements, and procedures.

C. <u>Administrative Requirements</u>[15]

1. Appoint a privacy officer;[16]

2. Designate a contact person or office responsible for receiving privacy-related complaints;[17]

3. Establish a plan workforce privacy training program under which all plan workforce members are trained in the policies and procedures designed to protect, as necessary and appropriate to carry out their work functions;[18]

4. Establish safeguards, including appropriate administrative, technical, and physical safeguards;[19]

5. Establish process for handling privacy-related plan member complaints;[20]

---

13. *See Id*. § 164.526.

14. *See Id*. § 164.528.

15. *See Id*. § 164.530. All of the administrative requirements described in the text above must be documented as specified under § 164.530(j).

16. *See Id*. § 164.530(a)(1)(i).

17. *See Id*. § 164.530(a)(1)(ii).

18. *See Id*. § 164.530(b).

19. *See Id*. § 164.530(c).

20. *See Id*. § 164.530(d).

6. Establish appropriate sanctions to be used against plan workforce members who violate the plan's privacy policies and procedures or the Privacy Standards;[21]

7. Mitigate harmful effects resulting from a violation of the plan's privacy policies and procedures or the Privacy Standards;[22] and

8. Establish policies and procedures for complying with the Privacy Standards.[23]

II. Privacy Standards Applicable to Employer Health Plans

A. Definition of "Health Plan"

1. "[A]n individual or group plan that provides, or pays the cost of, medical care."[24]

- "Health plan" includes "group health plans."
- "Group health plan" means an "employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), 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."

---

21. *See Id*. § 164.530(e).

22. *See Id*. § 164.530(f).

23. *See Id*. § 164.530(i). Covered entities also must refrain from intimidating or retaliatory acts against individuals and others for filing complaints and exercising their rights. *Id*. § 164.530(g). A covered entity may not require individuals to waive their rights as a condition to treatment, payment, enrollment in a health plan, or eligibility for benefits. *Id*. § 164.530(h).

24. 45 C.F.R. § 164.501 (citing definition in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

- The group health plan must have 50 or more participants or be a plan of any size that is administered by an entity other than the employer that established and maintains the plan.[25]

B. Firewall Requirements

1. Introduction.

- HIPAA applies to health plans, not plan sponsors;

- For this reason, the requirements focus on plans, and force plans to impose certain requirements on plan sponsors.

Neither employers nor group health plan sponsors are "covered entities" under HIPAA. Instead, HIPAA applies to health plans. Under ERISA, a group health plan must be a separate legal entity from its plan sponsor. Usually, this is evidenced by plan documents. As noted by DHHS, however, employers and other plan sponsors (particularly those sponsors with self-insured group health plans) may perform certain functions that are integrally related to or similar to the functions of group health plans. While carrying out these functions, the sponsors often require access to PHI held by the group health plan.[26]

DHHS recognized that, in the real world, ERISA-covered group health plans usually do not have a corporate presence. In other words, they may not have their own employees. Often, the only tangible evidence of the existence of a group health plan may be the contractual agreement or other plan documents that describe the rights and responsibilities of covered participants, including the benefits that are offered and the eligible recipients.[27]

According to DHHS, the Privacy Standards recognize plan sponsors' legitimate need for health information in certain situations, while at the same time the Standards recognize the need to protect health information from being used for employment-related functions or for other functions related to other benefits provided by the plan sponsor. DHHS states that:

---

25. *Id*. § 164.501.

26. 65 Fed. Reg. 82462, 82507 (December 28, 2000).

27. *Id*.

> "We do not attempt to directly regulate employers or other plan sponsors, but pursuant to our authority to regulate health plans, we place restrictions on the flow of information from covered entities to non-covered entities."[28]

Consequently, the Privacy Standards permit group health plans (and allow them to authorize insurers and HMOs with respect to the plan) to disclose PHI to a plan sponsor if the plan sponsor agrees to use and disclose the information only as permitted or required by the regulations. In particular, the PHI may be used only for plan administration functions performed on behalf of the group health plan and which are specified in the plan documents.[29] Plan sponsors may not access PHI for employment-related actions or in connection with any other benefit or employee benefit plan.[30]

2. **Plan Documents**. Under Section 164.504(f), unless an exception applies (including plan member authorizations), a group health plan may disclose PHI to a plan sponsor only if the plan documents restrict uses and disclosures of such information by the plan sponsor as described below.

3. **Exceptions**. Plan documents need not be amended when only the information described below (for the purposes described below) is given to the plan sponsor:

   - Group health plans may give plan sponsors "summary health information" for (a) obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or (b) modifying, amending, or terminating the group health plan;

     and

28. *Id.* at 82508.

29. *Id*.

30. *Id*.

- Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurer or HMO offered by the plan.[31]

4. **Specific Plan Document Amendments**. When plan amendments are required as specified above, the amendments must incorporate provisions to establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures are not inconsistent with the Privacy Standards.

- Plan documents must state that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsors agrees to:

- Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

- Ensure that any agents, including a subcontractor, to whom it provides PHI received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

- Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

- Report to the group heath plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

- Make available protected health information in accordance with § 164.524;

---

31. 45 C.F.R. §164.504(f)(1)(iii). "Summary health information" means information that may be individually identifiable health information and that summarizes the claims history, claims expenses, or types of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan. Certain identifiers must be deleted, except that the geographic information described in § 164.512(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code. *Id*. § 164.504(a).

- Make available PHI for amendment and incorporate any amendments to PHI in accordance with § 164.526;

- Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

- Make its internal practices, books and records relating to the use and disclosure of PHI received from the group health plan available to DHHS for purposes of determining compliance by the group health plan with the Privacy Standards;

- If feasible, return or destroy all PHI received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purposes for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible;[32] and

- Ensure that "adequate separation" between the plan sponsor and group health plan is established by:

  - Describing those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the PHI to be disclosed, provided that any employee or person who receives PHI relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

  - Restricting the access to and use by such employees and other persons described above to the plan administration functions that the plan sponsor performs for the group health plan; and

  - Providing an effective mechanism for resolving any issues of noncompliance by those persons.[33]

32. 45 C.F.R. § 164.504(f)(2)(ii).

33. *Id*. § 164.504(f)(2)(iii).

5. Group Health Plan Uses and Disclosures. Group health plans may:

- Disclose PHI to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the Standard regarding plan document amendments;

- Not permit a health insurer or HMO with respect to the group health plan to disclose PHI to the plan sponsor except as permitted by the Privacy Standards;

- Not disclose and may not permit a health insurer or HMO to disclose PHI to a plan sponsor as otherwise permitted by the Standards, unless a statement required by § 164.520(b)(1)(iii)(C)[34] is included in the appropriate notice; and

- Not disclose PHI to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.[35]

C. Employment Records

1. In the final modifications to the Privacy Standards, DHHS clarified that employment records are not considered PHI. When an employee gives medical information to a covered entity as the employer (including a doctor's statement to document sick leave), for example, the medical information becomes part of the employment record and as such, is no longer considered protected health information. The covered entity, however, may be subject to other laws and regulations.[36]

Employment records therefore may contain medical information needed for the employer to carry out its obligations under FMLA, ADA, and similar laws, as well as files or records regarding occupational injuries, disability insurance eligibility, sick leave, drug screening, workplace medical surveillance, and fitness-for-duty test of employees. Although this type of information contains

---

34. The required statement: "A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan." 45 C.F.R. § 164.520(b)(1)(iii)(C).

35. *Id*. § 164.504(f)(3).

36. 67 Fed. Reg. 53182, 53192 (August 14, 2002).

identifiable health information, it is obtained by a covered entity in its capacity as employer, and will not be considered protected health information.[37]

D. Insured Plans

1. Group health plans that provide health benefits solely through an insurance contract with a health insurer or HMO, and that do not receive PHI (other than summary and enrollment/disenrollment information), are exempt form many of the Privacy Standards.[38] In particular insured plans that do not receive PHI are exempt from the Standards relating to:

- Appointment of a privacy official;
- Designating a contact person responsible for receiving complaints and providing further information;
- Plan workforce training;
- Safeguards;
- Complaints;
- Workforce Sanctions;
- Mitigation;
- Policies and Procedures.[39]

2. These types of plans also do not need to produce a notice of privacy practices.[40] In the preamble to the December 28, 2000 final rule, DHHS noted that these types of insured plans also are exempt from patient rights requirements (access, amendment and accounting), since these

---

37. *Id*.

38. 45 C.F.R. § 164.530(k)(exempting such plans from § 164.530(a) through (f) and (i)).

39. *Id*.

40. *Id*. § 164.520(a)(2)(B). Insured plans that create or receive PHI (in addition to summary health and enrollment/disenrollment information) must maintain a notice and provide it upon request. *Id*.

plans do not have access to PHI.[41] "Individuals enrolled in a group health plan that provides benefits only through an insurance contract with a health insurance issuer or HMO would have access to all rights provided by this regulation through the health insurance issuer or HMO, because they are covered entities in their own right."[42]

The preamble to the December 2000 final rule mentions that these types of insured plans must comply only with the documentation requirement in § 164,530(j) and "only with respect to plan documents amended in accordance with § 164.504(f)."[43] This is confusing, however, because plan documents do not have to be amended if the plan sponsor does not receive PHI from the group health plan (or from a health insurer or HMO on behalf of the plan).

Many insured plans do not receive PHI from the insurer/HMO, but certain plan sponsor employees nonetheless receive PHI from plan members when assisting them in navigating the insurance system and/or advocating on their behalf with insurers/HMOs. When such plan sponsor employees receive PHI from plan members, would the "plan" fall within the insured plan exemption described above? *This is unclear*. If the plan sponsor employees who assist plan members with claims obtain authorizations from plan members and do not use the PHI disclosed for any other purpose, it is possible that the plan may still fit within the insured plan exemption.

Any plan sponsor of an insured plan that wishes to take this approach should consider establishing policies and procedures designed to limit (1) the plan sponsor employees who will be involved with such claims assistance activities; and (2) the uses and disclosures of PHI such plan sponsor employees receive during this process. These plan sponsor employees should remain outside the plan firewall. Plan document will not need to be amended under § 164.504(f) if the plan sponsor

---

41. 65 Fed. Reg. 82462, 82645 (December 28, 2000).

42. *Id*.

43. 45 C.F.R. § 164.530(k)(2); 65 Fed. Reg. at 82564. The regulations do not explicitly exempt insured plans from complying with § 164.530(g) and (h) (refraining from intimidating or retaliatory acts and the prohibition on requiring individuals to waiver their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits).

employees obtain signed authorizations from plan members when assisting them with claims.

III. Practice Issues

A. Assist Clients in Developing a Group Health Plan Privacy Action Plan

1. **Phases**. List phases of HIPAA implementation, including:

   - Assessment/Inventory;
   - Strategic Analysis;
   - Implementation.

2. **Specific Tasks and Personnel/Department Assignments**. Include specific tasks and list the person who will be responsible for such tasks, including following the flow of plan member PHI, determining what vendors constitute business associates, and re-contracting with business associates.

B. Initial Documents Needed For Group Health Plan Compliance

1. Inventory/Assessment Questionnaires -- optional;
2. Plan document amendments, if applicable;
3. Notice of Privacy Practices, if applicable;
4. Policies and Procedures;
5. Forms/Logs, including authorization forms and accounting disclosure logs.

C. Policies and Procedures

1. **What Policies?** The types and number of policies and procedures will differ among employer group plans, depending upon a number of factors, including but not limited to the nature of the business, and whether the group health plan uses a third-party administrator. The policies listed below are an attempt to develop a minimum list of policies. Some group health plans may develop many more policies. Others may have a number of policies addressing one of the topics below. For example, the Plan Member Rights policy may be broken

down into separate policies addressing each plan member right separately.

2. **Overall Privacy Policy Addressing Handling of PHI and "Adequate Separation."** All plans need this type of policy and the place to start is with the required plan document amendments. This policy must be consistent with these requirements, but should be more readable and may be used to train plan workforce members. For example, this policy should list the employees (by position) who will have access to PHI and the level of such access. For this reason, this policy may address the "minimum necessary" standard. Alternatively, this standard may be addressed in a separate "minimum necessary" policy. This policy also could address organizational issues, including affiliated entities and organized health care arrangements, if applicable.

3. **Other Possible Group Health Plan Policies and Procedures**:

   - Plan Member Rights Policy (detailed);
   - Plan Member Privacy Complaints Policy;
   - Plan Workforce Training Policy;
   - Privacy-related Plan Workforce Sanctions Policy;
   - Safeguards for Protecting PHI Policy;
   - Plan Documentation and Retention of Certain Records Policy;
     - This policy would address retention of HIPAA policies and procedures and documentation of certain tasks, including documenting member rights requests and responses, and certain administrative (e.g., appointment of a privacy official). The Privacy Standards do not address retention of claims and other records containing PHI. If the client desires, this policy may address that issue as well.
   - Policy on Authorizations (including forms).

D. <u>Training Policy Drafters</u>

1. Consider training policy drafters before they start drafting the policies.

- Avoid overly broad, absolute pronouncements about privacy and security;
    - "Your records will be kept completely confidential."
    - "We never release your records without your permission."
- Avoid extraneous detail, including historical information about previous policies;
- Avoid overstating protections and safeguards -- generally avoid stating that the Plan or a particular Plan Workforce member "ensures" the privacy or security of PHI;
- Allow flexibility for practice variation and innovation if permitted under the Privacy Standards;
- Do not adopt a policy or procedure that will not be, or is not capable of being, implemented;
    - For example, do not pick a shorter time frame than that required by the Privacy Standards unless this time frame can be accomplished easily. If clients insist on this, list these shorter timeframes as "goals."
- Consider requiring legal review of all policies.
    - HIPAA is not just a project; it is the law. The policies and procedures must comply with the Privacy Standards.

E. Selected Issues

1. Telephone inquiries from spouses/children/others regarding a member's claims/benefits:

- Authorization is required;
    - Does Section 164.510 help? Does a plan want to "exercise professional judgement [when individual not present] to determine whether the disclosure is in the best interest of the

individual?[44] Will plan workforce members know all the facts, e.g., marital separation, custody dispute?

- Recognize that the Privacy Standards focus on individuals, not groups of plan members associated with a particular employee/subscriber.

- Significant Systems Issues;

  - Many customer service information systems were designed to focus on the employee/subscriber *and* his or her associated dependents as a group.

- Customer Service Issues;

  - Some plan members may be accustomed to easy access to their spouse's information.

- Creative Solutions;

2. Who are Plan Employees?

- Consequences/potential liability related to wearing two hats;

- Mitigating risks by implementing meaningful training and sanction programs;

- Mitigating risk by having clear policies and procedures.

3. Re-negotiation of Third-Party Administrator Agreements.

- Add required business associate terms;

- Consider adding/modifying other related terms; often, much more than the required terms will be necessary to accomplish HIPAA compliance objectives;

- Transition period, if applicable.

---

44. *See* 45 C.F.R. § 164.510.

4. **Self-funded plans that want to delegate everything to a TPA**.

   - Can the plan delegate all HIPAA responsibilities and liabilities? No.

   - Dealing with disbelief -- careful client counseling.

5. **Real Risks: Penalties and Litigation**.

   - The compliance date (April 14, 2003) approaches for plans that are not small health plans;

   - Small health plans have until April 14, 2004;

   - Civil and criminal penalties;

   - Case Law: *U.S. v. Sutherland* -- a federal judge was persuaded that the Privacy Standards "demonstrate a strong federal policy of protection for patient medical records." The judge applied the HIPAA regulations to that case (involving a health care provider, not a health plan), significantly before the compliance date;[45]

   - Is there a new "standard of care" for how health plans/employers should handle PHI?

45. *United States v. Sutherland*, 143 F. Supp. 2d 609 (W.D. Va. 2001) (www.vawd.uscourts.gov/opinions/jones/sutherland1.pdf); see also *United States ex rel. Stewart v. Louisiana Clinic*, 2002 U.S. Dist. LEXIS 24062 (E.D. La. December 11, 2002).