HISCOCK & BARCLAY LLP

HIPAA Fundamentals: HIPAA for the Small to Mid-Size Employer

Ninth Annual HIPAA Summit
Baltimore, MD
September 14, 2004

Melissa M. Zambri, Esq.
Hiscock & Barclay, LLP

50 Beaver Street
Albany, New York 12207
(518) 429-4229 (Phone)
(518) 427-3463 (Fax)
mzambri@hiscockbarclay.com
www.hiscockbarclay.com

The Problems with HIPAA Implementation for Small to Mid-Size Employers

1) Limited resources for HIPAA implementation
2) Person organizing benefits may have numerous other responsibilities
3) Harder to create a firewall because of small size
4) Confusion about rules in press - many myths including:
   - Only self-insured plans need to be concerned
   - Every plan must comply with all of the requirements
   - A plan can pass off all of its responsibility to a third party administrator (TPA)

HIPAA Application to Employers

"We cannot regulate employers." Employment records are specifically excluded from the definition of protected health information (PHI). The Department did not define the term "employment record." However, it did clarify that medical information needed for an employer to carry out its obligations under the FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees, may be part of the employment record.

HIPAA Application to Employer-Sponsored Health Plans

Generally, health plans are covered entities, where 50 or more participants or administered by a third party other than the plan sponsor, including, but not limited to:

- Medical Plans
- Dental Plans
- Vision Plans
- Health Flexible Spending Accounts

Questions to Ask

Question #1: Is the health plan self-insured or fully-insured?

Meaning of fully-insured – benefits solely through an insurance contract with an insurer or an HMO. This would be the situation for most small to mid-size employers.

Question #2: If the plan is self-insured, the company often seeks to remember why it decided to self-insure.

Self-insured plans are subject to the numerous requirements of the rules.

Question #3: If the plan is fully-insured, does the benefits department really want PHI?

Fully-insured plans are exempt from many of the administrative requirements of the privacy rules if the plan only receives summary health information and participation/enrollment/disenrollment information. Note that there is no exception for fully-insured plans in the security rules.

Exemption for Fully–Insured Plans

Fully–insured plans that only receive summary health information and participation/ enrollment /disenrollment information have limited responsibilities. They are not required to:

- Have a Privacy Officer
- Train
- Develop Safeguards
- Establish a Complaint Procedure
- Sanction for Violations
- Mitigate
- Create Policies and Procedures
- Provide Rights to Participants
- Provide a Notice

However, They Must Still:

- Refrain from Intimidating or Retaliatory Acts
- Not Require a Waiver of Rights
- Maintain Any Amendment to the Plan Document for the Required Time Period
- Execute a Business Associate Agreement, if Applicable
- Comply with the Security Rules

Information Used by Plan

- Summary Health Information is a subset of PHI (may be individually identifiable health information) that summarizes claims history, expense, or experience and has been stripped of certain personal identifiers.
- What is my organization doing that requires more than summary health information or participation/enrollment/disenrollment information and do I really want/need to get that information?

  In-house benefits personnel may be performing functions which require access to PHI, i.e. interacting with health insurers and TPAs regarding issues where the interaction includes the exchange of PHI; eligibility determinations; collecting and tallying medical receipts under flexible spending accounts; monitoring utilization, etc.

The Issues With Flexible Spending Accounts/Cafeteria Plans

- Probably cannot use “fully-insured” concept.
- Cannot pass on covered entity status or responsibilities.
- Can get assurances from business associates and try to keep PHI out of the plan’s possession but duties and sanctions will rest with the flex or cafeteria plan, as the covered entity.
- Those plans with under 50 participants often use a TPA.
- Bringing function back in-house provides the flex/cafeteria plan with information that the medical plan is trying to refrain from receiving.

Information to Plan Sponsor

Unless the plan documents are amended, plan sponsors may only receive summary health information, where its use is limited to obtaining premium bids for insurance coverage and modifying, amending or terminating the plan, and participation/enrollment/disenrollment information.

If the plan sponsor receives additional information or summary health information for other purposes, it must:

- Amend plan documents and provide certification to the plan
- Establish proper uses and disclosures
- Disclose PHI only as permitted by the plan documents or required by law
- Not use or disclose PHI for employment-related actions or decisions or in connection with another benefit
- Separate plan from employer, including reasonable and appropriate security measures – specifically carve out who needs access to PHI, restrict access accordingly (firewalls), and have a plan for violators

If the plan sponsor receives additional information or summary health information for other purposes, it must: (cont.)

- Ensure that agents agree to the same restrictions and employ reasonable and appropriate security measures
- Report improper uses or disclosures and security incidents
- Allow access, amendment and provide for accounting
- Allow Secretary to review records
- Return or destroy information when no longer needed if feasible; protect it if not
- Implement reasonable and appropriate administrative, physical and technical safeguards to protect electronic PHI

Privacy Rule Requirements Where Can't Take Advantage of Fully–Insured Exception

If 1) a fully-insured plan gets more than summary information and participation/enrollment/disenrollment information, or 2) the plan is self-insured or a flex/cafeteria plan, plan must:

- Appoint a privacy officer
- Establish policies and procedures
- Safeguard PHI
- Allow participants to exercise rights
- Train
- Sanction
- Provide notice
- Take complaints
- Maintain documentation
- Refrain from intimidating or retaliatory acts
- Mitigate harm if violation occurs
- Execute business associate agreements
- Undertake security rule compliance, including administrative, physical and technical safeguards

Business Associate Issues

Optional Language to Look For:

1. Requiring the Business Associate to Have a *Written* Privacy and Security Plan
2. Injunctive Relief
3. Indemnification
4. Termination if Business Associate Violates HIPAA with Another Customer
5. Assistance in Judicial or Administrative Proceedings

Policies and Procedures

Limited time and resources. Our policies and procedures for a small to mid-size company cover the following, as applicable:

- Confidential Communications and Requesting Restrictions
- Special State Requirements (for example, in New York, HIV/AIDS information)
- Computerized Information
- Faxed, Photocopied and Written Materials
- Oral Communications
- Authorization
- De-Identification

Policies and Procedures (cont.)

- Minimum Necessary With List of Job Titles and Information Required
- Disclosures Required by Law
- Business Associates
- Training
- Access, Amendments, Accountings
- Sanctions
- Documentation
- Notice of Privacy Practices
- Family and Friends
- Privacy Officer
- Complaint Policy
- Verification of Persons
- Violations

Policies and Procedures (cont.)

Document should be complete enough to be meaningful but compact enough to be workable.

Should be scaled to the size of the organization.

Conclusions

1. Careful analysis required of what information flows within a health plan and outside of the plan for all employers that sponsor health plans.
2. The best approach may be the least employee-friendly.
3. The best approach may reduce chances of discrimination-type suits.

The top 10 questions I get asked by small to mid-size employers

10. Am I supposed to know what HIPAA is about?
9. Do I really have to care?
8. I read somewhere that I have to do all of this stuff to comply with HIPAA. Is it true?
7. What if I haven't done anything yet?
6. So, wait, my flex plan has under 50 participants, if I didn't hire the TPA to administer the flex plan, I wouldn't have to comply? Should I bring it back in-house?
5. If I am fully-insured, why am I getting a business associate agreement?
4. Can I not send flowers to an employee who is in the hospital anymore?
3. We make widgets. How come I am talking to a health lawyer?
2. I thought it had something to do with administrative simplification?
1. Why me?

WHAT ARE YOUR QUESTIONS?