Agent 77

HIPAA Overview for Employer-Sponsored Health Plans

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a sweeping set of federal legislation and regulations created to improve the portability of an individual's healthcare coverage when changing jobs and to promote administrative simplification of health insurance.

Title I of the law, effective since 1996, provides for improved health insurance access and portability when changing jobs. This aspect of HIPAA has affected the benefits of over 3 million Americans.

HIPAA's administrative simplification regulations affect healthcare practices, clearinghouses and health plans, including insurance companies, HMOs and employer-sponsored health plans. These regulations require standardized electronic transactions, improved privacy and security methods, and greater access to, and rights for, individuals regarding their health information.

Who Does HIPAA Affect?

HIPAA affects health care providers, healthcare clearinghouses and health plans, including insurance companies, HMOs and employer-sponsored health plans. HIPAA's Administrative Simplification rules govern the actions of covered entities' in the areas of transactions, privacy and security. All covered entities are subject to the Act.

Covered entities under HIPAA[i] include health plans which are defined as "An individual or group plan that provides, or pays the cost of, medical Under HIPAA health plans include:

1. Group Health Plans with more than 50 eligible participants or which are administered by someone other than the sponsoring organization
2. HMOs, long-term care insurers, and state-licensed health insurance companies
3. An employee welfare benefit plan offering or providing health benefits to the employees of two or more employers
4. Federal and State health benefit programs[iii]
5. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

Most health plans offered by employers (including those which pay for medical, dental, vision, chiropractic, behavioral health or other health care, as well as medical reimbursement or other types of medical payment) are included in the definition above. The covered entity governed by HIPAA is the health plan itself, not the employer. **As the sponsor of the plan, it is the responsibility of the employer to ensure that the plan complies with all applicable regulations.**

What Do I Have To Do To Comply?

HIPAA includes three sections with which health plans must comply: transactions, privacy and security. Compliance involves:

Conducting transactions in a certain way (directly or through a TPA or insurance company)
Protecting member privacy to new, uniform levels and providing members access to their records
Ensuring security of physical and electronic member records

HIPAA was created to ensure uniformity in the application of transactional, privacy and security standards across the health care industry. It requires not only that you meet certain standards in

these areas, but insists that you document your policies, procedures and how you continue to meet these standards for each individual.

Once an organization determines that it is a covered entity, HIPAA compliance is required by statue. Compliance with the Transaction and Security rules is required for all covered entities. However, under the Privacy rule there are several classes of compliance requirements. Within the broad definition of health plans, HIPAA provides exceptions to Privacy requirements for some types of plans.

Level 1 Plans
Health plans that (1) "provide[s] health benefits solely through an insurance contract with a health insurance issuer or HMO", and (2) only receive enrollment/disenrollment status and summary data[iv] must only meet two simple tests to comply with HIPAA[v]:

(1) They must agree not to discriminate against their enrollees on the basis of any medical condition or whether a member files a HIPAA grievance; and
(2) They must agree not to ask their enrollees to waive their HIPAA rights.

These plans rely on the insurance carrier or HMO to provide notification and most of the HIPAA rights to their enrollees. In fact, HIPAA automatically creates a special relationship between a Level 1 plan and the carrier or HMO, in which all policies, forms, the Notice of Privacy Practices, etc. created by the carrier automatically apply to the employer-sponsored plan. Additional compliance with the Transactions and Security regulations is required. However, their impact will be minimized due to the low level of protected health information maintained by these plans.

Level 2 Plans
Health plans that (1) "provide[s] health benefits solely through an insurance contract with a health insurance issuer or HMO", and receive enrollment/disenrollment status and detailed data[vi] may rely on the carrier/HMO to provide certain notices, but they are required to meet almost all HIPAA responsibilities (see below) including amending plan documents, maintaining a Notice of Privacy Practices, designating a privacy officer, etc. These plans must also certify to the carrier/HMO to that carrier's satisfaction that they are HIPAA compliant. Transactions and security regulations also apply fully.

Level 3 Plans
Any other health plan for which the prior exemptions are not applicable must comply with all HIPAA transactions, privacy and security regulations. The most common of these plans is self-funded, meaning that the employer pays for the cost of medical care directly, not through an insured relationship.[vii] **However, any plan which does not "provide[s] health benefits solely through an insurance contract with a health insurance issuer or HMO" must comply with all HIPAA requirements, including provision of a notice of privacy practices, Privacy Officer, over 35 policies and procedures, over 30 forms, use of authorizations, etc.**

To comply with the Privacy rules, Level 2 and 3 plans need to take numerous steps, including the development and implementation of more than 60 policies, procedures, forms and job descriptions, as well as:

- Modifying plan documents
- Designating who may access Protected Health Information
- Establishing firewalls
- Creating and implementing policies and procedures
- Certifying to your carrier/HMO that you are HIPAA compliant
- Issuing a Notice of Privacy Practices
- Identifying Business Associates and getting agreements from each
- Tracking certain types of member information requests for six years
- Allowing members to amend their medical records
- Allowing members to restrict access to certain medical information

What Happens if I Don't Comply?

HIPAA is the law. Non-compliance carries serious penalties, including:

- $100 per incident, up to $25,000 per standard, per year, in civil penalties for privacy standard violations.
- Federal criminal penalties for the intentional misuse of protected health information up to $250,000 and 10 years in prison.

Enforcement is expected to complaint driven. Member and employees can report violations to the Office of Civil Rights within the Department of Health and Human Services. Ignorance is expensive; even the civil penalties can add up quickly.

In addition, HIPAA compliance represents an excellent defense against frivolous wrongful termination suits. HIPAA Privacy and Security are the standard against which the actions of plans and employers are expected to be judged.

When Do I Have To Comply?

HIPAA is already the law of the United States and is in effect today. However, the required compliance date for health plans depends on the size of the plan.

If your plan has more than $5 million in claims or premiums:

- Transactions – October 16, 2002. (10/16/03 with extension)
- Privacy – April 14, 2003
- Security – April 21, 2005

If your plan has less than $5 million in claims or premiums:

- Transactions – October 16, 2003
- Privacy – April 14, 2004
- Security – April 21, 2006

What Do I Do Next?

The HIPAA regulations encompass well over 1,500 pages and, even then, do not provide a detailed description on how to comply. Those interested in setting up a compliance plan and all of the policies, procedures, job descriptions, forms, and everything else for HIPAA compliance on their own could face hundreds of hours of work and thousands of dollars in cost.

Thankfully, an easy solution is available. Built just for employer-sponsored health plans like yours, Agent 77's HIPAA*Now!* Toolkit provides CD-ROM-based training, a comprehensive Guide and Workbook and customer service to give you all the tools you need to make your practice HIPAA compliant. The HIPAA*Now!* Toolkit makes HIPAA compliance as "easy as A-B-C."

For more information on the easiest, most cost-effective solution for complying with ALL the HIPAA compliance requirements, contact Agent 77 or your benefits professional for more information about Agent 77's HIPAA*Now!* for Health Plans Toolkit. It contains everything you need for compliance: all of the written policies, procedures, forms, and other documents required by the law (there are over 60 of them), as well as easy-to-follow step-by-step instructions on how to make your organization compliant with HIPAA.

Our customers' experience has shown that, depending on the complexities of your health plans, a company using the Toolkit can complete all the necessary compliance activities in **16-24 hours** (2-3 working days full-time). And our free customer support gives you toll-free telephone access to experts you can talk to when you have questions. Compare that to the **hundreds of hours** compliance can take by doing it yourself or with other tools, and you can see why over 2,500 customers are using HIPAA*Now!* today.

HIPAA compliance can be easy, cost-effective, and stress-free! Contact Agent 77 at (866) 629-6500 or your benefits professional for more information on HIPAA*Now!* for Health Plans.

Endnotes:

[i] Federal Register, Vol. 65, No 160 (Aug 17, 2000) Pages 50365-50366.
"Covered entity means one of the following:
(1) A health plan
(2) A health care clearinghouse
(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."

[ii] Federal Register, Vol. 65, No 160 (Aug 17, 2000) Page 50366. The full definition includes 16 types of health plans, summarized in the text above as 5 types. See the Federal Register for a full list in the original order.

[iii] Federal and State health benefit programs include:
1. Medicare
2. A Medicaid program
3. A Medicare supplement issuer
4. The health plan for active military personnel
5. The veterans health care program
6. CHAMPUS
7. The Indian Health Service
8. The Federal Employees Health Benefit
9. A state child health plan
10. The Medicare+ Choice program

[iv] "Summary data" is data with sufficient data removed to identify the owner on its face. Specifically, § 164.504 Uses and disclosures: Organizational requirements of HIPAA states: *Summary health information* means information, that may be individually identifiable health information, and:
(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and
(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

[v] See HIPAA § 164.530(g-k)

[vi] Detailed data is any claims or other PHI where the indicated identifiers have not all been removed, and therefore at least one is present. See HIPAA § 164.530(g-k)

[vii] From the Minnesota Office of the Ombudsman for Mental Health and Mental Retardation website:
"Under self-funding, the employer, rather than paying a premium to an insurance company and transferring risk, will opt to pay employee health care claims directly out of company assets."