

Davis Wright Tremaine LLP

LAWYERS



Practice Areas: Healthcare - eHealth/HIPAA

advisory bulletins

Home

Practice Areas

eHealth/HIPAA:

[Legal Services](#)

[Related Practice Areas](#)

[Advisory Bulletins](#)

[Publications & Resources](#)

[Events and Meetings](#)

[eHealth/HIPAA Search](#)

News to Use

Recruiting

DWT in the Community

Seminars & Training

Bookstore

Lawyer Directory

Office Locations

Search & Site Map

Advisory Bulletin

[return to Advisory Bulletin page](#)

A Road Map for Employer Compliance With HIPAA

■ [download Advisory Bulletin as .pdf](#) (93K)

By Keith M. Korenchuk, Rebecca L. Williams, Stuart W. Miller, Jason T. Froggatt, Gerald M. Hinkley
[April 2002]

How employers, health care providers, and health plans treat health care information is undergoing a dramatic transformation in the United States. Congress passed the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") in response to requests for standardization of the health care payment process.

When first enacted, the media and health care industry focused their attention on HIPAA's insurance portability and anti-fraud provisions; HIPAA's administrative simplification, including security and privacy provisions, initially escaped notice. Despite the deluge of attention now focused on administrative simplification, many employers are still unaware that HIPAA will have a significant impact on their operations, particularly their employee benefit plans. The deadline for compliance with HIPAA's privacy regulations is April 2003.

Employers need to assess current operations, determine HIPAA's applicability, and develop a plan for HIPAA compliance. To assist with the compliance process, this article sets forth a basic framework for that assessment, as well as highlights the important provisions of HIPAA as they pertain to employers.

THE REQUIREMENTS OF HIPAA

HIPAA's administrative simplification provision covers three key categories of requirements: transactions standards, which mandate that health care claims and related "transactions" be processed using standard format and content (with an effective date as late as October 2003 if a request is filed); privacy provisions, which require elaborate policies, procedures, and systems with respect to maintaining and releasing health information (effective in April 2003); and security requirements (final regulations are expected to be published sometime in 2002 with compliance mandated 26 months later). HIPAA directly covers:

- Health plans (including a wide variety of employer-sponsored group health plans),
- Health care providers who transmit HIPAA transactions electronically, and
- Health care clearinghouses that process or facilitate processing of non-standard data elements into standard data elements or vice versa.

Interestingly, employers as a class are not covered entities (unless they otherwise fall into one of the above-described categories).

Under HIPAA, a covered entity generally may not use or disclose protected health information, except: (1) for treatment, payment, or health care operations (in compliance with HIPAA requirements), (2) upon the individual's agreement in certain limited situations (after an opportunity to agree or object), (3) to the individual, subject to his or her rights under HIPAA, (4) as permitted or required by HIPAA (for governmental or other purposes), or (5) pursuant to an authorization from an individual.

Additionally, HIPAA grants certain rights to individuals, such as the rights to access, amend, and receive an accounting of disclosures of their protected health information. HIPAA also imposes certain administrative responsibilities on covered entities.

Protected health information includes individually identifiable health information transmitted or maintained in any form or medium. This individually identifiable information encompasses a long list of personal information relating to an individual that either identifies or can be used to identify that individual.

DETERMINING HIPAA'S IMPACT ON EMPLOYERS - AN APPROACH

By its very depth and breadth, HIPAA likely will have a major impact on employers who provide or arrange for health care benefits for their workforce. Assessing this impact requires a multi-part analysis:

(1) Is the employer a covered entity under HIPAA? This determination needs to be made with reference to the definition of "covered entity" in the privacy regulations. Those definitions then must be compared to the activities undertaken by an employer. Most employers, themselves, will not be deemed to be a provider, health plan, or health care clearinghouse and, therefore, not a covered entity. To the extent an employer operates a health care clinic for its employees, as a small part of its operations, the employer likely will be a hybrid entity under HIPAA.

(2) If so, what are the employer's obligations under HIPAA? If the employer does qualify as a covered entity, then it will need to implement the HIPAA requirements applicable to its type of covered entity. A covered entity that is a hybrid entity will need to ensure that its health care component separately complies with the applicable HIPAA requirements.

(3) Is the employer's employee benefit plan a covered entity? A covered health plan includes a group health plan, which is defined as an employee welfare benefit plan under ERISA. This may include hospital and medical benefits plans, dental plans, vision plans, health flexible spending accounts, and employee assistance plans. Both insured and self-insured plans are covered to the extent that the plan provides medical care to employees and/or their dependents. An exception exists for a plan with less than 50 participants that is self-administered. Most employers, however, will have plans with 50 or more participants or that are administered by a third party, such as a third party administrator or TPA. Therefore, most employer-sponsored benefit plans will be covered entities under HIPAA.

(4) If so, what are the plan's HIPAA obligations? The specific HIPAA requirements need to be identified and a compliance plan developed and implemented for the covered plan.

(5) If an employer is not a covered entity but its benefit plan is, what other obligations does the employer have as a plan sponsor or plan fiduciary? Most employers will not be classified as a covered entity under HIPAA but will find themselves classified as a plan sponsor and potentially subject to the obligations of a plan sponsor under HIPAA. Moreover, under the ERISA default rule, plan sponsors are deemed to be the plan administrators of their plans and, thus, are fiduciaries of the plan. As fiduciaries, plan sponsors likely have an obligation to ensure their plans are compliant, regardless of any direct obligations imposed by HIPAA. This creates a two-fold role for employers. First, the employer will need to ensure that any covered plans comply with the applicable HIPAA requirements. It may be prudent to enter into discussions with and receive assurances from any TPA or insurance carrier involved with the plan concerning its HIPAA compliance activities. Second, the employer that wants or needs access to its plan's protected health information will need to comply with the plan sponsor requirements.

OBLIGATIONS OF COVERED ENTITIES

If the employer or its employee benefits plan is deemed to be a covered entity, then it will need to comply with applicable HIPAA requirements. HIPAA imposes different requirements depending on whether the covered entity is a plan, a provider, or a clearinghouse. It is possible for a single entity to engage in activities that make it a combination of covered entity types. A covered entity will need to specifically identify its particular obligations under the HIPAA privacy regulations based on the type of functions it performs, as well as requirements for standard transactions, security, and other administrative simplification provisions.

As plan sponsors or plan fiduciaries, most employers will need to implement on behalf of their covered benefit plans, or ensure that the insurance provider implements, the requirements HIPAA imposes on covered health plans.

Such covered plans need to comply with HIPAA's standard transactions by October 16, 2002, or file a request and a compliance plan with the Department of Health and Human Services (HHS) prior to that date to obtain a one-year extension.

On the privacy side, plans will need to develop policies, procedures, and systems to address appropriate uses and disclosures of protected health information. Under the "minimum necessary" rules, covered entities must develop approaches to ensure that only those workforce members with a need to know use or access such information.

HIPAA privacy regulations implement certain individual rights including the right to access, amend, receive an accounting of disclosures, complain, and request additional protections, subject to certain limitations. Moreover, HIPAA mandates certain administrative requirements.

The HIPAA privacy regulations obligate covered entities to provide privacy awareness training for all workforce members, including volunteers, trainees, and non-employees whose work is under the direct control of the covered entity. That training must be fully documented. Covered entities should include security awareness training in that program, incorporating password management, incident reporting, and anti-virus software and protections. The training must be job-specific and given to new employees "within a reasonable period of time" after they join the workforce. Covered entities must design policies

and procedures that fully comply with HIPAA's privacy and security requirements.

Human resources policies and job descriptions should be modified to incorporate privacy and security obligations. There also must be a system of "appropriate sanctions" for workforce members who fail to comply with privacy and security policies and procedures and a system of monitoring and evaluating such compliance.

A privacy official must be named. Responsibility for developing and implementing those policies and procedures must be vested in a trained and qualified privacy official.

Covered entities also must identify third parties with which it discloses protected health information. Such third parties may qualify as business associates. Accordingly, covered entities will need to negotiate and enter into business associate contracts.

OBLIGATIONS OF EMPLOYERS AS PLAN SPONSORS

Most employers, as plan sponsors, will want to comply with a variety of provisions under HIPAA with respect to how they handle protected health information and how their health plan documents need to be amended. An assessment must be made of how the employer, as a plan sponsor, handles employee health care information, whether the employer needs access to this information, and whether the information gathered by the employer qualifies as protected health information under HIPAA.

Most employers have and want access to their plans' protected information, such as for adjudication purposes. HHS has stated that major employers, with more than 200 employees, are likely to hold or gather protected health information, making them subject to HIPAA's plan sponsor requirements. In addition, HHS forecasts that significant numbers of employers with less than 200 employees are likely to have access to protected health information as well. Most employers acting as plan sponsors, therefore, will want to comply with HIPAA's plan sponsor requirements.

To the extent that an employer is a plan sponsor, that its plans are deemed covered group health plans, and that it obtains protected health information from the covered plans, then it will need to amend its group health plan documents, agree to comply with such documents, and make certain assurances. Before a group health plan can disclose protected health information to its sponsor, it must include provisions in the plan documents to establish permitted and required uses and disclosures of protected health information by the plan sponsor. In short, the plan is permitted to disclose protected health information to the plan sponsor only to carry out plan administration functions. The plan document must provide, and the plan sponsor must certify, that the plan sponsor will:

- Not use or further disclose protected health information, other than as permitted by the plan documents or as may be required by HIPAA.
- Ensure that agents or subcontractors of the plan sponsor who receive plan protected health information agree to comply with the same restrictions.
- Not use or disclose this information for employment- related actions or in connection with other employee benefit plans.
- Report to the health plan any use or disclosure of the information that is inconsistent with

- permitted uses or disclosures.
- Make protected health information available to plan participants, consider their requests for amendments, and, upon request, provide them with an accounting of disclosures of their protected health information to third parties
- Make documentation and internal practices available to HHS upon request.
- Return or destroy protected health information received from the health plan that the sponsor maintains in any form, with no copies to be retained, if feasible, or ensure continued protections if not feasible.

Additionally, a group health plan must include a statement in its notice of privacy practices that it may disclose protected health information to its plan sponsor. To ensure that an adequate separation exists between the plan and the plan sponsor, the plan documents also must:

- Describe the class of employees of the plan sponsor who are given access to protected health information of the plan.
- Restrict access to, and use by, plan sponsor employees in plan administration to functions that the plan sponsor performs for the health plan.
- Provide a procedure for resolving issues of non-compliance.

All of these changes must be made in the plan documentation prior to the compliance date of the HIPAA privacy regulations, which currently is April 14, 2003, for most plans.

EMPLOYER HIPAA ACTION PLAN

To begin the compliance process, employers should take the following steps:

(1) Conduct a covered entity analysis of employer. Determine if the activities of the employer and its work force qualify the employer as a covered entity under HIPAA. If so, compliance with the HIPAA privacy, transaction, and security requirements will be required. If an employer is not a covered entity, compliance with the plan sponsor provisions still will likely be required.

(2) Conduct a covered entity analysis of its employee benefit plans. Evaluate whether the employer's employee benefit plan falls within the definition of a group health plan. If so, the plan will be deemed a covered entity under HIPAA and must comply with applicable HIPAA requirements including privacy, security, and standard transactions.

(3) Conduct an information flow assessment. Conduct an assessment of how the employer obtains protected health information from employees and its benefit plans, how it uses that information in administering the employment and plan relationship, and what categories of employees have access to such information. Along a similar track, the flow of protected information to, from, and within the employer's group health plan must be evaluated. If no protected health information is used or disclosed, no further changes for the non-covered employer (as opposed to its covered plans) are required under HIPAA. Most employers, however, will collect this information for their plans and will need to meet the plan sponsor requirements of HIPAA.

(4) Perform a gap analysis. Evaluate whether current actions, information flow, and documentation are consistent with HIPAA requirements.

(5) Develop a remediation plan. Once this assessment of the current situation and the gap analysis are completed, a remediation plan for both the plan and the plan sponsor must be developed.

(6) Amend health plan documents. Company health plan documents must be amended to reflect the changes set forth above. The plan's documents may need to be negotiated and amended with the health care plan itself as part of this process.

MEETING THE HIPAA CHALLENGE

Many employers are not aware that HIPAA may dramatically impact their operations and activities, even though employers are not specifically designated as covered entities. Employers must begin to sort through the analytical process of determining the nature of their relationship with their employee benefit plans, their use of protected health information, and how their activities must be modified to ensure compliance with HIPAA. Because the HIPAA clock is ticking quickly, employers should begin this process as soon as possible.

ABOUT THE AUTHORS

[Keith M. Korenchuk](#) is a partner in DWT's Washington, D.C. office. Keith is Co-Chair of the firm's Health Law Department and Chair of the Global Alliance for eCommerce Law, the first alliance of major independent law firms around the world focusing on eCommerce and the Internet. He is an experienced practitioner in the area of health law and advises many health care systems, health care companies, medical groups, hospitals, and managed care companies throughout the United States.

Keith can be reached at (202) 508-6616 or keithkorenchuk@dwt.com.

[Rebecca L. Williams](#), a partner in DWT's Seattle office, is an experienced registered nurse and serves as Co-Chair of the firm's HIPAA Task Force. Her practice involves HIPAA, anti-kickback, Stark, tax-exemption, compliance, patient care, and other regulatory issues as well as transactions and contracting. She is the author of several published articles and book chapters on health law and is a national speaker on health care issues. Becky is a contributing editor to the Employee Benefits Institute of America's HIPAA & Other Federal Mandates for Group Health Plans.

Becky can be reached at (206) 628-7769 or beckywilliams@dwt.com.

[Stuart W. Miller](#) is a partner in DWT's San Francisco office. Stuart's practice focuses on employment and labor law and litigation, including leaves of absence, sexual harassment and wage and hour issues. In addition to this publication, he co-authors DWT's California Employment Law Advisory Bulletins.

Stuart can be reached at (415) 518-8367 or stuartmiller@dwt.com.

[Jason T. Froggatt](#) is an associate in DWT's Seattle office. Jason's main focus is employee benefits. He is a frequent speaker on employee benefits compliance issues as well as the author of the "Taxation of IRA's and Qualified Plan Distributions" chapter of the Washington Lawyers Practice Manuals.

Jason can be reached at (206) 628-7629 or jasonfroggatt@dwt.com.

[Gerald M. Hinkley](#) is a partner in DWT's San Francisco office and a member of the firm's Health Law Department. His practice centers primarily on health care regulation and joint ventures, startups, mergers, acquisitions and strategic alliances, Internet transactions, managed care and financing transactions involving organizations in the health care industry, including hospitals, health care systems, clinics, physician organizations, insurers and health plans, senior housing operators and nursing homes. He is an experienced negotiator and strategic advisor. Gerry is active in numerous professional organizations, including the American Health Lawyers Association and the Health Care Financial Management Association. He is also the founder of the Bay Area Health Care Breakfast Club.

Gerry can be reached at (415) 276-6530 or at gerryhinkley@dwt.com.

This Health Law Advisory is a publication of the Health Law Group of Davis Wright Tremaine LLP. Our purpose in publishing this Advisory is to inform our clients and friends of developments in health care law. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.

[return to Advisory Bulletins main page](#)

Davis Wright Tremaine LLP

[Home](#) | [Practice Areas](#) | [News To Use](#) | [Recruiting](#) | [DWT in the Community](#)
[Seminars & Training](#) | [Bookstore](#) | [Lawyer Directory](#) | [Office Locations](#) | [Search & Site Map](#)

Davis Wright Tremaine LLP

Copyright 1996-2002, Davis Wright Tremaine LLP, ALL RIGHTS RESERVED.
[Site Disclaimer](#), [Privacy Policy](#) & [Legal Information](#)

