Wiggin & Dana

Wiggin & Dana LLP
Counsellors at Law

One Century Tower
P.O. Box 1832
New Haven, Connecticut
06508-1832
Telephone 203.498.4400
Telefax 203.782-2889

One CityPlace
185 Asylum Street
Hartford, Connecticut
06103-3402
Telephone: 860.297.3700
Telefax: 860.525.9380

400 Atlantic Street
P.O. Box 110325
Stamford, Connecticut
06911-0325
Telephone: 203.363.7600
Telefax: 203.363.7676

June 11, 2002

New Federal Requirements For Health Plans

HIPAA's Impact on Employers

New technology has transformed the way society manages information, but has also raised significant privacy concerns, particularly in relation to confidential personal matters such as health information. You may have heard about recent regulatory attempts to improve privacy protections for such information, but you should be aware that ***employers*** *are also exposed to these regulations, in their roles as sponsors and administrators of employer group health plans. Planning for compliance now will allow you to adapt your health plans to meet these requirements, and avoid the significant penalties for wrongful disclosures, without disrupting your ongoing business.*

Federal regulations issued in 2000 pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will require sweeping changes in the way health plans manage the health information of participants and beneficiaries. These so-called "Administrative Simplification" requirements of HIPAA primarily address three separate components: 1) electronic transactions and code sets; 2) privacy; and 3) security. The electronic transactions and code sets regulations, known as the Electronic Data Interchange (EDI) Rule, establish national standards for certain electronic transactions such as claims, payment and remittance advice, and enrollment. Compliance with the EDI Rule generally involves coordination with one or more software vendors and the testing of compliance capability. While plans that engage in electronic transactions originally had to be in compliance with the EDI Rule by October of 2002, Congress granted a **one-year extension** for those plans that by October 15, 2002, file a Compliance Plan that addresses the reason for the extension request, the work plan to achieve compliance, and plans to begin testing by April 16, 2003. If these requirements are applicable to your group health plan, a straightforward model Compliance Plan and instructions for submitting it electronically are available at the HHS HIPAA web site, www.cms.gov/hipaa.

The privacy component of the Administrative Simplification provisions, which is set forth in detailed regulations known as the "Privacy Rule," dramatically changes how health plans and health care providers use and disclose health information. The Privacy Rule compliance deadline is less than one year away (April 14, 2003; April 14, 2004 for plans with

annual receipts of $5 million or less). Given the comprehensive nature of these requirements, health plans should begin planning for compliance now. While the requirements of the Privacy Rule may seem onerous, they serve as an opportunity for health plans to improve operations and administrative efficiency. The remainder of this advisory outlines the general obligations that the Privacy Rule places on plans and plan sponsors, and describes a number of implementation steps to consider in light of the new regulations. Regulations on the HIPAA security component are yet to be finalized.

The Privacy Rule in a Nutshell

Generally, the Privacy Rule regulates the use and disclosure of "protected health information" (PHI). PHI is *any* individually identifiable health information that is transmitted or maintained in any form. The Privacy Rule only applies to "covered entities," a term which is broadly defined to include:

- Group health plans (insured or self-insured) that have 50 or more participants *or* plans of any size that are administered by an entity other than the plan sponsor. Group health plans include medical, dental, vision, health care flexible spending account and prescription drug plans, and mental health programs
- health insurance issuers
- HMOs
- Medicare
- Medicaid
- Medicare-supplemental policy issuers
- 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
- Health programs for active military personnel and veterans
- the Indian Health Service
- the Federal Employees Health Benefits Program
- Medicare+Choice plans
- an approved state child health plan
- state high risk pools
- any other individual or group plan that provides or pays for the cost of medical care.

In addition, the Privacy Rule regulates health care providers and health care clearinghouses. These "covered entities" cannot use or disclose PHI unless permitted or required by the Rule, or unless the individual authorizes the use or disclosure of the PHI.
Employers and plan sponsors are *not* covered entities. However, where an employer sponsors a self-insured, or partially self-insured plan, the

employer becomes directly responsible for the "covered entity" (i.e., the employer group health plan) and, thus, the burden of compliance will fall on the plan sponsor.

Employers whose group health plans are fully insured should not be lulled into thinking that they do not need to take any action to ensure HIPAA compliance, believing that their insurers will be solely responsible for compliance. The extent to which such employers need to concern themselves with HIPAA compliance depends on the extent to which the employer needs protected health information that is in more than summary or "de-identified" form. (See discussion below).

Life insurance, long- and short-term disability, and workers' compensation plans and programs are not covered entities. As a result, the Privacy Rule does not apply to them directly. However, a health plan that is a covered entity may not disclose PHI to these programs without an individual authorization (unless required by law). The converse is not true, however. For example, if an employer sponsors a disability plan and has obtained an independent medical exam in connection with the administration of the disability plan, the examination report may be disclosed without authorization by the disability plan to the employer's group health plan, but the group health plan may not disclose PHI to the administrator of the disability plan.

The Good News

Health plans *can* use or disclose PHI, without authorization, for "treatment, payment, and health care operations". Payment and health care operations would include things such as determinations of coverage, billing, quality assessment, utilization review, and business planning and development. If the health plan contracts with outside service providers to carry out any functions that involve the use of PHI, such as claims processing or administration, data analysis, or utilization review, the health plan can also disclose PHI to these service providers, and permit them to use and disclose PHI. Before PHI can be disclosed, however, employer group health plans must contractually obligate service providers to comply with the Privacy Rule. These service providers are known as "business associates," and contracts between health plans and business associates must meet certain requirements, including setting out the permitted uses and disclosures of PHI, and providing that the business associate will comply with the Privacy Rule (including permitting the Secretary of HHS and the covered entity to have access to its records for audit purposes) and report any violations of the Privacy Rule to the covered entity.

The Bad News

Any uses or disclosures of PHI for reasons other than treatment, payment, or health care operations (whether in-house or by a business associate), require an authorization from the individual who is the subject of the PHI unless another specific provision of the Privacy Rule allows the use or disclosure (such as to government agencies overseeing the health plan, or in response to court orders). In order to be effective, an authorization must meet the specific requirements of HIPAA.

In addition, the Privacy Rule guarantees certain rights to individuals whose PHI is maintained by an employer group health plan. For instance, individuals must be allowed to inspect and copy their own information, and may request an amendment of the PHI in the health plan's records. Health plans must track uses and disclosures of an individual's PHI, and give individuals an accounting of these disclosures on request. Health plans are also required to explain their uses and disclosures of PHI in a Notice of Privacy Practices, which must be provided to all participants no later than the compliance date, at the time of enrollment for new enrollees, and within 60 days of any material change to the Notice. Health plans will be required to designate a privacy official, train employees on how to handle PHI, and provide a procedure to address complaints (as outlined below, fully insured employer group health plans that do not disclose any PHI to the plan sponsor are exempt from these "administrative" requirements). Finally, even if a use or disclosure is permitted under the Privacy Rule, employer group health plans must make reasonable efforts to limit the PHI used or disclosed to the minimum amount necessary to accomplish the purpose (known as the "minimum necessary" rule).

Special Rules for Plan Sponsors

Key Privacy Rule provisions regulate when a plan sponsor can have access to PHI. Recognizing that sponsors (particularly in the case of self-insured plans) often need PHI in order for the plan to function, the Privacy Rule does contain a mechanism for such disclosures. Plan sponsors that receive PHI from the plan must meet more onerous requirements, however, and so employers must carefully consider whether they need access to PHI, or whether de-identified or summary health information will suffice for their purposes.

Self-Insured Plans

If a plan sponsor's employees perform any services for the plan that involve the use or disclosure of PHI on a basis that is not summary or de-identified, the plan documents must be amended to identify which employees will have access to PHI and the purposes for which PHI will

be used. This is the case *even if* these employees perform functions that fit under the definition of "treatment, payment, or health care operations" described above. The sponsor will also need to establish "firewalls" to ensure that any PHI is not used for employment-related decisions or other benefit plans. The plan sponsor must then "certify" to the plan that the required amendments have been made and that the sponsor has agreed to certain restrictions on the use and disclosure of PHI.

Typically employers sponsoring self-insured plans will have access to PHI that is not de-identified, whether from telephone conferences with third-party administrators, claim forms, plan audit reports, or claims appeals. It may be unrealistic for such a plan to operate with only summary or "de-identified" information. For this reason, some plan sponsors of self-insured plans may want to consider whether the advantages and cost-savings associated with self-insured plans outweigh the administrative burdens of complying with the HIPAA privacy regulations and the increased liability risks attendant to such compliance.

It should be noted that the Privacy Rule does allow the plan to disclose "summary health information" to the sponsor to carry out its settlor functions for such purposes as soliciting premium bids, or modifying or terminating the plan. If only summary information (information from which certain identifiers summarizing claims history and the like have been removed) is disclosed, the sponsor need not amend the plan documents. A plan sponsor also is permitted to perform enrollment functions on behalf of the plan without amending the plan documents. All covered entities also are allowed to disclose information that has been "de-identified," meaning information from which all potentially identifying data (including birth dates, five-digit zip codes, and account numbers) has been removed. If the plan sponsor's need for health information goes beyond these permitted disclosures, however, the plan documents must be amended. For instance, if the Benefits or Human Resources department of the plan sponsor handles the final level of appeal of a claims decision for a self-insured plan, and through this function has access to PHI, the plan documents will have to be amended to make this clear. Significantly, if a plan is amended in this fashion, participants will have a private right of action to sue under ERISA if they feel PHI has been improperly disclosed. The Privacy Rule itself does not contemplate suits by individuals.

Fully Insured Plans

As discussed above, while employers are not "covered entities" under the rule, fully-insured health plans still must comply with the Privacy Rule, although the insurance issuer or HMO will also be required to meet the

Privacy Rule's requirements. While employers with fully insured plans may not have a similar need for PHI, plan documents for such plans must also be amended if the plan sponsor wishes to have access to PHI that is maintained by the plan's insurer or HMO on a basis that is not summary or de-identified. If a group health plan (even a fully-insured one) receives more than summary health information from the health insurance issuer or HMO, the group health plan also must ensure the individual rights outlined above, and comply with the administrative requirements, such as designating a privacy official and providing the Notice of Privacy Practices. As is the case with self-insured plans, a health insurance issuer can disclose "summary health information" to the sponsor without the need for plan amendment, and the sponsor can also perform enrollment functions without such amendments.

While a fully-insured plan need not enter into a Business Associate contract with the insurer or HMO, the plan will still need to ensure that the HMO or insurer (a covered entity in its own right) is complying with the Privacy Rule, including the individual rights provisions. Employers with fully-insured plans should also determine whether all the benefits offered by the plan (such as vision, dental, and mental health) are actually fully insured, because the Privacy Rule applies to these "plans" as well.

Whether or not an employer with a fully insured plan needs to access PHI on a non-summary basis depends on the particular circumstances of the employer. The employer may need such PHI for on-going benefits litigation, in order to administer its wellness programs, or because the employer is involved in some level of claims appeals.

Common Misconceptions about HIPAA

While the Privacy Rule is lengthy and complex, the purpose of the Rule is simple – HHS sought to protect the confidentiality of health information maintained by health plans and other covered entities, and so health plans must adopt certain procedures to ensure that any uses or disclosures of this information are permitted by the Rule. The sheer volume of the regulation should not overwhelm plans, or cause them to postpone compliance efforts. With assistance and proper advance planning, most plans should be able to handle the transition to compliance with the Privacy Rule and other HIPAA requirements with relative ease. Plans should not think, however, that they can avoid having to comply with the regulations by contracting with a third party administrator (TPA). TPA's are not "covered entities" under the Privacy Rule but are, instead, "business associates" of the plan. The compliance obligation therefore rests with the group health plan. Given that the civil penalties can range up to $25,000 for each kind of violation, with criminal penalties increasing to $250,000 and/or ten years imprisonment, we strongly recommend that plans begin now to assess the implications of HIPAA.

Implementation Steps

Employer group health plans should take the following steps to assess the extent to which changes will be necessary under the Privacy Rule:

- Identify an individual or group of individuals who will be responsible for coordinating and leading your compliance effort.

- Look at the benefits offered by your plans and determine which benefit plans will be covered by HIPAA. Are they self-insured, fully insured, or partially insured?

- Inventory the PHI held by the group health plan or received from the group health plan. Who has access to the information? Where is it held? How is it used and disclosed? Why is it maintained? Determine how your organization uses PHI with respect to the plan, and if PHI is used for any other programs.

- Decide if summary health information is sufficient for your purposes, or if your organization will need to amend the plan documents to allow greater access to PHI of the plan's participants.

- Identify those vendors and partners of the health plan that may have access to PHI, including TPAs. Analyze these contracts and, if necessary, amend to meet the Privacy Rule's requirements.

- Collect and analyze all privacy policies and document retention policies.

- Consult with legal counsel regarding your organization's particular needs.

Conclusion

This advisory is a general summary of the Administrative Simplification requirements, and is not intended to address all of the regulations' provisions, nor is it tailored to your specific plans. Wiggin & Dana has a team of attorneys who can provide strategic and planning assistance as you prepare to comply with the new rules. If you would like more details about how the HIPAA Privacy Rule and EDI Rule may affect your plan's operation and administration, please contact Sherry Dominick (203) 498-4331, Chris Lindgren (203) 498-4348, or Jennifer Willcox (203) 498-4396.

Nothing in this Client Advisory *constitutes legal advice, which can only be obtained as a result of personal consultation with an attorney. The*

information published here is believed to be accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

Wiggin & Dana HIPAA Team

Jeanette Schreiber, HIPAA Practice Chair	203.498.4334	jschreiber@wiggin.com
Maureen Weaver, Health Care Department Chair	203.498.4384	mweaver@wiggin.com
Michelle Wilcox DeBarge	860.297.3702	mdebarge@wiggin.com
Catherine Baatz	860.297.3748	cbaatz@wiggin.com
Michele Gerrior	203.498.4585	mgerrior@wiggin.com
Mark Heaphy	203.498.4356	mheaphy@wiggin.com
Stacie Kelly	203.498.4369	skelly@wiggin.com
David Levenstein	203.498.4401	dlevenstein@wiggin.com
Jennifer Willcox	203.498.4396	jwillcox@wiggin.com

Wiggin & Dana Benefits Practice

Karen Clute	203.498.4349	kclute@wiggin.com
Sherry Dominick	203.498.4331	sdominick@wiggin.com
Christian Lindgren	203.498.4348	clindgren@wiggin.com

For more information visit www.HIPAA-law.info.