

What Every Employer Needs to Know About the HIPAA Privacy Rules

By Timothy J. Stanton, Kathleen S. Scheidt, and Sarah Bassler Millar

It finally happened!

The Privacy Rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") became effective for most employers on April 14, 2003 and will take effect April 14, 2004 for certain "small" plans.

By now most employers should have completed the initial planning steps - determining which parts of your organization are covered by the Privacy Rules; analyzing how your organization uses and discloses participant health information; reviewing contracts with administrative services companies; and appointing "privacy officials" to lead internal compliance efforts - and implemented your policies and procedures. Many employers with "small" plans (see the definition on page 2) are working on initial planning steps and will be moving into the implementation phase.

To assist employers with "small" plans in developing a strategy for being in compliance by April 14, 2004, and as a review for "large" plans, we have prepared this detailed question-and-answer guidance. This guidance incorporates the final version of the Privacy Rules and also draws on our experience advising clients on these issues over the past several years.

Our analysis is organized under 10 key subject headings- Covered Entities, Protected Health Information, Business Associates, Consents and Authorizations, Administrative Requirements, Individual Rights, Plan Amendments, "Minimum Necessary" Standard, Preemption, and Insured v. Self-Insured Plans. To make this Memorandum most useful for you, we have also included detailed lists of the requirements for many of the basic HIPAA compliance documents.

Covered Entities

One of the first questions you may ask in the course of HIPAA compliance planning is: what exactly is a "covered entity"?

The Privacy Rules cover three types of entities: health care clearinghouses; certain health care providers (those that transmit health information in standard electronic transactions); and "health plans," which are defined broadly enough to include health insurers and HMOs, various government medical programs, and employer-sponsored health benefit plans. The definition of health plan includes various types of benefit plans sponsored by any type of employer, such as medical, dental, vision, prescription drug, health flexible spending account, and long-term care plans, as well as most employee assistance plans.

A typical large employer might sponsor four or five separate plans that are "covered entities." Additionally, an employer-sponsored plan often will coordinate with an insurer or HMO to provide coverage to employees. The Privacy Rules ease the compliance burden on such group arrangements, called "organized health care arrangements." The covered entities participating in such arrangements are permitted to use and disclose information more freely with each other and may also issue a joint Notice of Privacy Practices to participants.

Is my company a "covered entity"?

Unless your employer is itself a clearinghouse or health insurer or provider, the rules do not apply directly to the employer. But the health benefit plans or programs your company sponsors may be covered entities.

Are all of my company's welfare benefit plans covered by these rules?

No. For example, long- and short-term disability plans, workers compensation benefits, life insurance plans, and sick pay programs are not covered by the Privacy Rules (even though they all involve employee health information). There is also a probably little-used exclusion from the "covered entity" definition for employer-sponsored health plans that are entirely self-administered and have fewer than 50 participants.

What's a small plan and why would it matter to a large company?

A "small health plan" is one with annual receipts of \$5 million or less. Small health plans can delay compliance with the rules until April 14, 2004. Even a large employer may have some plans (e.g., long-term care or vision) that are "small."

Protected Health Information ("PHI")

So what exactly is this PHI?

"Protected health information," or PHI, is another important concept to incorporate into your compliance effort because the Privacy Rules prevent health plans from using or disclosing a participant's (including a former participant's) PHI except as authorized by the regulations under HIPAA.

Generally, PHI is individually identifiable health information that is transmitted or maintained in any form or medium and that relates to the past, present, or future physical or mental health or condition of a participant, the provision of health care to a participant, or the past, present, or future payment for the provision of health care to a participant. Information is "individually identifiable" if it either actually identifies an individual or contains enough specific information to do so.

So all the health information that my company has about employees is PHI, right?

No. Only health information used or created by your company's health plans (or other covered entities) would be PHI. One significant change in the final rules is the addition of a specific exclusion from the definition of PHI for "employment records" held by a covered entity in its role as an employer. Though this language would be more reassuring to plan sponsors if the provision specifically mentioned employer health plans, it does indicate an acknowledgment that not all health information held by employers is affected by the Privacy Rules.

But if an employer is not a covered entity, should the employer have any health plan PHI at all?

Many employers would find it difficult, if not impossible, to administer health benefit plans without some of their employees having access to some PHI. This information can be shared with the plan sponsor if the PHI has been "de-identified," if it is merely enrollment information or "summary" claims information (that is not individually identifiable), or, more importantly, if your company certifies that it will comply with the Privacy Rules, takes the appropriate steps to do so, and amends its plan document as needed. In one useful change for employers, the final rules clarify that simple enrollment information is, in fact, PHI, but it can be shared between a plan and plan sponsor without the plan amendments summarized below.

Business Associates

Who are my plan's "business associates" and why does this label matter?

No matter how far along they are in their compliance efforts, many employers are finding that the impact on dealings with "business associates" is one of the most immediately tangible effects of the Privacy Rules.

Under the Privacy Rules, your plans cannot disclose plan PHI to their business associates without having in place a written contract that includes almost a dozen specific privacy protections. These business associate agreements are critical to fully safeguarding PHI when used or disclosed by service providers — such as third-party administrators, pharmacy benefit managers, benefit consultants, and attorneys — not otherwise covered by the Privacy Rules.

A services firm whose work includes using individually identifiable health information from your plan could be a "business associate" of the plan in one of two ways. First, it could perform *on behalf of the plan* any of a range of functions covered by the Privacy Rules (examples include claims processing, utilization review, and quality assurance). Second, it could provide *to the plan* one or more specific services (legal, actuarial, consulting, accounting, data aggregation, management, administrative, accreditation, or financial).

Business Associate Agreements

Under the Privacy Rules, a business associate agreement must:

- List the permitted and required uses and disclosures of PHI by the business associate;
- Prohibit the use and further disclosure of PHI other than as permitted or required by the contract or as required by law;
- Require the business associate to use appropriate safeguards to prevent uses or disclosures of PHI other than those allowed by the contract;
- Obligate the business associate to report to the plan any uses and disclosures which violate the contract;
- Require the business associate to ensure that its agents and subcontractors who are given plan PHI agree to follow the restrictions and conditions imposed on the business associate by the contract;
- Require the business associate to make available PHI for participant requests for access to, and amendment of, their PHI and accounting of disclosures of that PHI;
- Require the business associate to make its internal practices, books, and records relating to plan PHI available to DHHS for purposes of determining the plan's compliance with the Privacy Rules;
- State that the business associate will, if feasible, return or destroy all plan PHI, or, if such return or destruction is not feasible, extend the protection of the contract to such PHI and limit further uses and disclosures to those that make return or destruction infeasible; and
- Authorize termination by the plan if the business associate violates a material term of the contract.

What is the deadline for getting these new agreements in place?

These agreements could be entirely new contracts or just additions to existing agreements. The final rules provide very limited relief from the general requirement that an employer-sponsored health plan have a HIPAA-compliant business associate agreement in place by April 14, 2003. A written contract with a business associate that is in place by October 15, 2002, and is not renewed or modified by April 14, 2003, is deemed to comply with the Privacy Rules until it is either renewed or modified, or April 14, 2004, whichever is earlier.

Generally, if a contract is renewed or modified between October 15, 2002 and April 14, 2003, this transition relief is not available. But "evergreen" contracts, in which renewal is automatic without changes in terms, do qualify for this relief.

So this basically gives an employer-sponsored plan an extra year to comply. Right?

No, not really. This delayed compliance date gives plans less substantive relief than it might initially seem. During the transition period, plans must still allow participants to access and amend their PHI and to receive an accounting of

disclosures of that PHI, and plans must also give DHHS information as needed to determine compliance. Throughout this period, your plan also must mitigate (to the extent practicable) any harmful effect that is known to the plan, of a use or disclosure of PHI by a business associate in violation of the plan's policies or the Privacy Rules.

Consents and Authorizations

Are my plans required to obtain participant consents before using PHI?

No. Even under prior versions of the rules, health plans would not have had to obtain participant consent to use PHI for "payment, treatment, and health care operations" (a broadly defined phrase that encompasses most activities in which an employer-sponsored health plan is likely to engage). The final version of the Privacy Rules eliminates the consent requirement for all other covered entities as well.

Although consents are not required, some employers are opting to include in their enrollment forms some sort of acknowledgment by a participant that he or she is consenting to the use and disclosure of his or her information for plan administration purposes. Doing so reminds participants that such uses and disclosures are not prohibited under the Privacy Rules.

Even though covered entities do not need consents anymore, will my plans still need authorizations?

Plans must still obtain participant “authorization” for most uses and disclosures of PHI beyond “payment, treatment, and health care operations” of the plan. Participants generally can revoke an authorization at any time in writing. Your plan may condition enrollment or eligibility for benefits on a participant providing authorization only in very limited circumstances when authorization is sought for pre-enrollment underwriting purposes.

Many plans probably will not use PHI for purposes beyond “payment, treatment, and health care operations,” and so will not use authorizations on a large scale. However, one instance in which an authorization might be needed is where health plan PHI is used to administer other benefit programs, such as LTD plans.

Prior to the final modifications of the Privacy Rules, the authorization requirements differentiated between authorization requests made by covered entities and those made by individuals. The final rules incorporate some of the requirements that originally applied only to covered entity-initiated authorization requests and eliminate the distinction between covered entity requests and individual requests.

Authorization seems like a difficult way to use information on a large scale. What other options would my plan have?

Rather than use this cumbersome authorization process, employer-sponsored health plans that want to use PHI for something beyond payment, treatment and health care operations could consider using “de-identified” information. “De-identified” information is PHI that has been stripped of all identifying data that might enable someone to identify the person to whom the PHI applies. This could be done by means

Authorizations

To be valid under the Privacy Rules, an authorization must contain at least the following elements:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- The name or other specific identification of the person(s), or class of persons, for whom or to whom the covered entity may make the requested use or disclosure;
- A description of each purpose of the requested use or disclosure;
- An expiration date or an expiration event;
- The individual’s signature and the date (if the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual);
- A statement of the individual’s right to revoke the authorization in writing and either (i) the exceptions to the right to revoke, including a description of the revocation procedure, or (ii) if the revocation rights are described in the Notice of Privacy Practices (discussed below), a reference to the notice;
- An explanation of the plan’s ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the individual’s authorization, including the extent to which treatment, payment, enrollment, or eligibility may be conditioned on authorization and the consequences of an individual’s failure to provide authorization; and
- A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and then no longer will be protected by the Privacy Rules.

of an outside expert or a safe-harbor method that involves removing 18 direct identifiers ranging from name and address to biometric indicators.

As an alternative to full de-identification, the final rules also permit employer health plans to disclose information in a “limited data set.” A limited data set is PHI that excludes 16 of the 18 direct identifiers. These data sets would require an additional contract and are primarily designed for use in research. Employers that need only limited information from their health plans may be able to take advantage of the limited data set alternative. The use of limited data sets may slightly reduce the privacy compliance burden for such health plans, in part because the plans are not required to account to participants for disclosures of PHI in limited data sets.

Administrative Requirements

Do employers understand the importance of the administrative requirements in the Privacy Rules?

They might not. One common misconception about HIPAA compliance is that it requires not much more than adding some standard language to your contracts and distributing some standard communication materials to your participants.

To see why this is a misconception, you need only look at the administrative requirements. Of particular interest to benefits executives and in-house benefits counsel is the requirement that a plan designate a “privacy official” responsible for developing and implementing the plan’s privacy and procedures policies, and a “contact person” (who may also be the Privacy Official) to receive complaints and provide further information about those policies and procedures. Furthermore, a plan may not require participants to waive their right to file a DHHS complaint as a condition for the provision of treatment under, payment by, enrollment in, or eligibility for the plan. Additional administrative requirements are described below.

What is a “privacy policy,” and does my plan need one?

The Privacy Rules require plans to have policies and procedures to implement the administrative requirements and other parts of the rules. These policies would be for internal use and would describe a plan’s internal operations. There are not sets of required provisions for these policies, as is the case, for example, for notices of privacy practices, business associate agreements, and health plan documents.

Administrative Requirements

Beyond these personnel designations as noted above, the Privacy Rules also require your plan to:

- Train the employees who administer the plan on the plan’s privacy policies and procedures;
- Establish administrative, technical, and physical procedures that reasonably safeguard PHI from uses and disclosures that violate the Privacy Rules, including protection from incidental uses or disclosures made in connection with permitted or required uses or disclosures;
- Provide a process for participants to complain about your plan’s policies and procedures and its compliance with them;
- Establish and apply sanctions against employees involved in health plan administration when they violate the Privacy Rules or the plan’s procedures and policies;
- Mitigate, to the extent practicable, any known harmful effect of a use or disclosure of PHI in violation of your plan’s policies and procedures or the Privacy Rules;
- Refrain from intimidating, threatening, coercive, discriminatory, or other retaliatory action against an individual or others for the exercise of rights provided by the Privacy Rules or for participation in a process established by the Privacy Rules;
- Establish policies and procedures designed to safeguard PHI in compliance with the Privacy Rules; and
- Retain for six years copies of all privacy policies and procedures, written communications, and other records required to be documented by the Privacy Rules.

Will these administrative requirements about “incidental” uses and disclosures create problems for my plans?

The final rules clarify that there is no violation when an incidental use or disclosure occurs in connection with the intended use or disclosure — provided that a plan has in place reasonable safeguards to prevent such incidental uses or disclosures. This is relevant to employers, for example, where conversations between benefits administrators may be overheard.

What is the deadline to worry about for the administrative requirements?

The general compliance dates apply in this area as well, but compliance with the administrative requirements should be an ongoing process. For example, training must be provided to current employees performing plan administrative functions by April 14, 2003; to new employees hired after April 14, 2003 within a reasonable period of time after their date of hire; and to employees whose functions are affected by a material change in the plan’s policies and procedures within a reasonable period of time after the change becomes effective.

Individual Rights

How do the Privacy Rules create individual rights for plan participants?

No part of your HIPAA compliance effort is likely to have a greater impact on participants (or to produce more calls and e-mails from them) than your efforts to enable them to exercise their individual rights under the Privacy Rules. The Privacy Rules create three important rights — to access your PHI, to amend it, and to receive an accounting of disclosures made of it — and require covered entities to explain these rights in a Notice of Privacy Practices.

What sort of right to access information will participants have?

Participants have broad rights to access and copy their PHI that is part of the records maintained by or for the plan. Your plan must respond to requests for access to the information within 30 days and will have to provide access in the format requested unless such information is not readily producible. One 30-day extension is available if the plan needs additional time to respond and notifies the participant in writing of the reasons for the delay and the date by which the plan will respond. Your plan may deny requests for access, but in most

circumstances (except those delineated in the Privacy Rules) the plan must allow the requesting individual to have the denial reviewed by a health care professional who was designated by the plan to conduct such reviews and who did not participate in the denial.

How will participants be able to “amend” their PHI?

Participants also have the right to have your health plan amend their PHI as long as it is part of the records maintained by or for the plan. The plan must respond to requests to amend within 60 days, although the plan may extend its response time once by up to 30 days if it needs additional time to respond and notifies the participant in writing of the reasons for the delay and the date by which the plan will respond. There is greater flexibility to deny these requests (compared to requests for access), most interestingly on the grounds that the PHI on file is already “accurate and complete.” But if your plan denies a request, a participant may either file a statement of disagreement or request that the amendment request and denial be included with all future disclosures of the participant’s PHI. The plan may prepare a written rebuttal to a participant’s statement of disagreement. If it does, the plan must provide a copy of the rebuttal to the participant.

The Privacy Rules require your plans to document and retain the designated health records that participants may access or amend as well as titles of the individuals responsible for processing requests for access or amendment. In addition, the rules contain specific access and amendment request denial and review procedures and deadlines that your plans must communicate to participants.

What is an “accounting of disclosures”?

Participants have the right to receive once every 12 months, upon request and free of charge, an accounting of the disclosures of their PHI made by your health plans for up to six years immediately preceding the date of the request (this would not apply to disclosures made prior to April 14, 2003, and by a plan for treatment, payment, or health care operations, and disclosures authorized by the participant). An accounting must be written and must satisfy several requirements imposed by the Privacy Rules. Reasonable fees could be charged for additional accountings.

The Privacy Rules contain special accounting rules for multiple disclosures of PHI to the same person or entity for a single purpose as well as for research-related disclosures for 50 or more individuals.

Your plans must document and retain the information required to be included in a disclosure accounting, records of the accountings provided to individuals, and the titles of the persons responsible for receiving and processing requests for accountings.

Are these individual rights standards the same for insured and self-insured plans?

Though the standards are the same, insured plans may have an easier time complying with the access, amendment and accounting rules because insurance companies and HMOs are required to comply with the rules in their own right as covered entities. For employers with self-insured plans, it will be very important to work with your service providers to assign responsibility for responding to these requests and to coordinate efforts.

How are participants supposed to get information about these new rights?

Needless to say, with these important new rights available to your participants, you will be responsible for providing an explanation and telling participants how they can exercise these rights. The mechanism that the Privacy Rules use for this task is a sort of mini-SPD (in fact, many employers may consider simply incorporating this document into their SPDs). This “Notice of Privacy Practices” must be distributed to participants in your plan on or before the date the Privacy Rules take effect (April 14, 2003 for most plans) and to new participants as they enroll, and it will have to be updated to reflect changes in how your plan handles PHI.

Employer-sponsored health plans generally must also include a separate statement that the plan may disclose PHI to the sponsor of the plan.

What if a plan applies stricter limits on uses and disclosures than those set by law?

Your plan may elect to limit further the uses or disclosures that it would be permitted to make under the Privacy Rule. If it does so, the plan may describe its more limited uses or disclosures in its notice, although the plan may not limit its right to make a use or disclosure that is required by law or permitted to prevent or lessen a serious or imminent threat to the health or safety of a person or the public. If your plan wants to be able to apply a change in its more limited uses and disclosures to PHI created or received before it issues a revised notice, the plan must reserve the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains. The statement also must describe how the plan will provide individuals with a revised notice.

Aren't these notices going to be pretty unwieldy?

That is a risk, especially when incorporating them into an already long and detailed SPD. Recognizing this problem, DHHS has indicated that it would be appropriate to use a short summary of the notice attached to a longer, complete notice (i.e., a “layered” notice). One other useful device is a combined notice, which is permitted for a group of plans sponsored by one employer (remember, this is called, in HIPAA-speak, an “organized health care arrangement”).

Why would my plans want to have participants acknowledge that they received the notice?

You may hear references to some providers obtaining a patient’s written acknowledgment of receipt of the provider’s Notice of Privacy Practices. These acknowledgments reflect a change in the final rules, which require certain providers

Accounting of Disclosures

Except as otherwise provided in the Privacy Rules, an accounting must include the following for each disclosure:

- The date of the disclosure;
- The name of the entity or person who received the PHI and, if known, the address of such entity or person;
- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or, in lieu of such statement, a copy of a written request for disclosure by DHHS for compliance purposes or by another entity for a permitted purpose for which the Privacy Rules do not require the individual’s authorization (such as certain public health activities, law enforcement, and judicial and administrative hearings).

Notice of Privacy Practices

Your Notices of Privacy Practices should be written in easily understandable language and must contain the following terms:

- The following statement as a header or otherwise prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”
- A description of the types of uses and disclosures that the plan is permitted by the Privacy Rules to make, including at least one example and sufficient detail to place the participant on notice of such uses and disclosures, for each of the following purposes: treatment, payment, and health care operations.
- A description of the other purposes for which the plan is permitted or required by the Privacy Rules to use or disclose PHI without the participant’s written consent or authorization, including sufficient detail to place the participant on notice of such uses and disclosures.
- If a use or disclosure for any treatment, payment, health care operations, or other permitted purpose not requiring authorization is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law.
- A statement that other uses and disclosures will be made only with the participant’s written authorization and that the participant may revoke such authorization.
- A statement of the participant’s rights with respect to PHI and a brief description of how the participant may exercise the rights to:
 - Request restrictions on certain uses and disclosures of PHI, including a statement that the covered entity is not required to agree to a requested restriction;
 - Receive confidential communications of PHI;
 - Inspect and copy PHI;
 - Amend PHI;
 - Receive an accounting of disclosures of PHI; and
 - Obtain a paper copy of the notice from the plan upon request even if the participant previously agreed to receive the notice electronically.
- A statement that the plan is legally required to maintain the privacy of PHI and to provide participants with notice of its legal duties and privacy practices with respect to PHI.
- A statement that the plan is required to abide by the terms of the notice currently in effect.
- A statement that the plan reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains, as well as a description of how it will provide participants with a revised notice.
- A statement that participants may complain to the plan and to the Secretary of DHHS if they believe their privacy rights have been violated, a brief description of how the participants may file a complaint with the covered entity, and a statement that the participant will not be retaliated against for filing a complaint.
- The name or title and telephone number of a person or office to contact for further information.
- The effective date of the notice, which may not be earlier than the date on which the notice is printed or otherwise published.

(but not health plans such as yours) to make a good-faith effort to obtain these acknowledgments. Your plans may wish to obtain participants' acknowledgments that they received the notice as a way to document your compliance with the Privacy Rules.

Plan Amendments

Do all plan documents have to be amended?

Unless nobody at your organization will be receiving any PHI (except enrollment information or aggregate "summary" claims information from which nearly all identifiers have been removed), you will need to make fairly extensive plan amendments. These plan amendments make it clear that not only must the plan safeguard PHI, but you, as plan sponsor, also must do so if you wish to use and disclose your plan's PHI.

Did you say "firewall"?

Actually, yes. The Privacy Rules require your health plans to ensure "adequate separation" between the plans (which probably have PHI) and the rest of your company's operations. The preamble to the rules borrows the computer security term "firewall." The "firewall" that separates your other business operations from your health plan is critical to safeguarding the plan's PHI. The policy and provisions establishing this

firewall must: (i) describe which employees will have access to PHI; (ii) restrict this access to plan administrative functions; and (iii) provide a way to resolve any violations of the policy by these employees.

"Minimum Necessary" Standard

What is the "minimum necessary" standard?

One of the biggest HIPAA privacy compliance wildcards for employers is the "minimum necessary" standard. Under this standard, your plan and its business associates must take reasonable steps to limit each use or disclosure of PHI to the minimum necessary use or disclosure to accomplish the relevant task.

How are my plans supposed to determine the minimum necessary use or disclosure?

The Privacy Rules, even the final version, contain little guidance about how a plan is supposed to determine whether any particular use or disclosure is actually the minimum needed to do the job. But the Privacy Rules are clear in requiring your plan to develop and implement policies and procedures appropriate for your company's business practices and workforce that are designed to minimize the amount of PHI that is used, disclosed, and requested. Plan documents and employee communications, internal procedures, and

Plan Amendments

The Privacy Rules require your plan document to:

- Identify the permitted and required uses and disclosures of PHI;
- Require the employer to certify that the plan document has been amended and the employer agrees to comply with these new provisions;
- Prohibit the use or disclosure of PHI other than as permitted or required by the plan documents or as required by law;
- Require agents and subcontractors who receive PHI to abide by the same restrictions and conditions that apply to the plan and the employer;
- Prohibit use of PHI for employment-related actions or in connection with any other benefit plans;
- Require the employer to report to the plan any improper use or disclosure of PHI;
- Give participants access to their PHI and enable them to amend it upon request;
- Provide participants, upon request, an accounting of all disclosures of their PHI;
- Make available to DHHS all internal practices, books, and records relating to the use and disclosure of plan PHI;
- Require the employer, once it no longer needs PHI for its intended purpose (*e.g.*, setting plan premiums), to return or destroy all copies of the PHI or, if this is not feasible, to limit further uses and disclosures; and
- Establish a "firewall" to ensure separation between health plan operations and the employer's other operations.

administrative arrangements must be updated to incorporate the minimum necessary standard as reflected in the plan's privacy compliance policies and procedures.

So, does this standard apply to everything the plan does?

Most things, but not all. The Privacy Rules clarify that the standard does not apply to certain uses and disclosures, such as those required by law, disclosures made to an individual pursuant to that individual's authorization, disclosures to and requests by health care providers for treatment purposes, and incidental disclosures as long as the disclosing party uses reasonable safeguards and has implemented minimum necessary standards. Therefore, health plans may disclose PHI that is reasonably necessary for workers' compensation purposes because the Privacy Rules specifically permit disclosure of PHI if the disclosure is legally required. In informal guidance, DHHS has helpfully stated that it does not intend the minimum necessary standard to interfere with best industry practices and it views this as a reasonable and flexible standard.

The efforts of your health plans to establish "minimum necessary" policies and procedures should begin with a survey of the types of PHI used in plan administration and the types and degree of PHI disclosures. Plan administrators may find that some functions can be performed adequately with fewer or less extensive uses or disclosures.

Preemption

How does HIPAA preemption of state law work?

Generally, the Privacy Rules will preempt state laws that are contrary to the Privacy Rules. But there is one specific exception that is potentially very important for employer-sponsored health plans: "more stringent" state laws may not be preempted. If your plan operates in a state that has more stringent laws that would apply to the operations of an **employee benefit plan** (*i.e.*, that would not be preempted by ERISA), your Notice of Privacy Practices must explain the more stringent state law protections.

What about old-fashioned ERISA preemption? Won't that protect my plan from these state laws?

HIPAA preemption is another compliance wildcard for employers, but one that will likely come into play only in future years and future state privacy laws. DHHS has indicated that it did not intend the Privacy Rules to replace the current ERISA preemption scheme. Still, it remains to be seen whether

states will — in the interest of medical record privacy — enact laws that will affect benefit plan administration, and how courts would react to such laws.

Insured vs. Self-Insured Plans

Do insured plans have some sort of free pass from the Privacy Rules?

No. Compliance generally may be easier for insured plans because insurance companies and HMOs are themselves covered entities, but the same rules usually apply.

However, the Privacy Rules do provide a limited exception for group health plans that provide benefits solely through an insurance contract (including a contract with an HMO). Two important forms of relief are available for such fully insured plans *if the plans do not create or receive any PHI, except "summary" information and enrollment/disenrollment information.* First, insured plans will not have to comply with most of the administrative requirements under the Privacy Rules and may not have to amend their plan documents. Second, these plans will not be required to provide or maintain a Notice of Privacy Practices because the insurer or HMO will be doing so.

Do many plans meet this standard?

Our sense is that insured plans sponsored by large employers often may receive more PHI than this exception would allow, though some employers may alter their procedures to try to take advantage of this exception. And even employers that provide benefits only through insured plans and receive little or no PHI could decide to take precautionary steps like appointing a privacy official or training employees in properly handling PHI.

Please feel free to contact any Employee Benefits attorney in the Gardner Carton & Douglas HR Law team listed below with any questions or concerns you may have.

HR LAW TEAM EMPLOYEE BENEFITS

| | |
|--|----------------|
| Kathleen O'Connor Adams koconnor_adams@gcd.com | (312) 569-1306 |
| Marla B. Anderson manderson@gcd.com | (312) 569-1314 |
| Gregory K. Brown gkbrown@gcd.com | (312) 569-1296 |
| Lisa L. Collins lcollins@gcd.com | (312) 569-1079 |
| Barbara A. Cronin bcronin@gcd.com | (312) 569-1297 |
| Ralph E. DeJong rdejong@gcd.com | (312) 569-1261 |
| Gary W. Howell ghowell@gcd.com | (312) 569-1299 |
| Jonathan Hyun jhyun@gcd.com | (312) 569-1315 |
| Nathan W. Johnson njohnson@gcd.com | (312) 569-1302 |
| Ann M. Kim akim@gcd.com | (312) 569-1303 |
| Howard J. Levine hlevine@gcd.com | (312) 569-1304 |
| Joyce L. Meyer jmeyer@gcd.com | (312) 569-1305 |
| Sarah Bassler Millar smillar@gcd.com | (312) 569-1295 |
| Michael D. Rosenbaum mrosenbaum@gcd.com | (312) 569-1308 |
| Mary K. Samsa msamsa@gcd.com | (312) 569-1309 |
| Kathleen S. Scheidt kscheidt@gcd.com | (312) 569-1310 |
| Lori L. Shannon lshannon@gcd.com | (312) 569-1311 |
| Timothy J. Stanton tstanton@gcd.com | (312) 569-1312 |
| Carol Hines Wacaser chines@gcd.com | (312) 569-1298 |
| David L. Wolfe dwolfe@gcd.com | (312) 569-1313 |

Gardner Carton & Douglas is a Limited Liability Company

This client memorandum is not intended as legal advice, which may often turn on specific facts. Readers should seek specific legal advice before acting with regard to the subjects mentioned here.

www.gcd.com