Gardner, Carton & Douglas
Client Memorandum
February 2001
HR LAW
Service to Our Clients and Our Friends

An Employer's Guide to the HIPAA Privacy Rules

Led by the newly created position of 'privacy official,' employers will need to make major changes to self-insured health plan documents, contracts and administration

By Timothy J. Stanton and Lisa L. Collins

Sweeping new health information privacy rules under HIPAA may soon make employers yearn for the relative simplicity of special enrollment, certificates of creditable coverage and the other parts of HIPAA designed to make health benefits more portable.

These new privacy regulations, issued by the Department of Health and Human Services ("HHS") on December 20, 2000, interpret the general privacy standard of HIPAA – that entities covered by the rules may not use or disclose individually identifiable health information unless either the covered entities have obtained the appropriate form of permission from that patient or the use or disclosure is expressly allowed by HIPAA.

Employers, as a whole, are not generally covered under the rules. However, most employers have components such as self-insured health plans they sponsor that *are* subject to the rules. Such employers are deemed to be "hybrid entities" for purposes of HIPAA. The HIPAA privacy regulations will affect the use and disclosure of protected health information ("PHI") by the health plan component of the employer and the corresponding workforce.

These new rules will require the self-insured health plan component of the employer (i.e., you the employer in your role as plan sponsor) to:

- Amend health plan documents to include more than a dozen specific privacy provisions.
- Negotiate or revise written contracts with third-party administrators, insurers, HMOs, managed care vendors and other "business associates" to incorporate more than a dozen specific privacy provisions.
- Appoint a privacy official who will be responsible for training employees involved in plan administration in handling PHI, and for ensuring that adequate privacy practices and procedures are in place.
- Protect participants' right to inspect and copy their PHI, amend the records, file complaints about them and receive an accounting of all disclosures of their PHI by the plan.
- Obtain detailed authorization from any participant whose PHI is to be used for any purpose other than "payment, treatment, and health care operations."
- Separate health plan administration where PHI must be maintained separately from other general corporate functions and even from the administration of other ERISA benefit plans.

The rules — which take effect ***February 26, 2003***, for health plans generally, and a year later for small health plans with annual receipts of $5 million or less — apply to *all* medical records and other individually identifiable health information maintained or disclosed by your health plan. In proposed form, the rules applied only to electronically transmitted information. The final version applies to *all* information, whether electronic, written and oral.

As if that wasn't enough to get employers' attention, the privacy provisions of the HIPAA statute generally carry significant penalties. Civil penalties range up to $100 per person, per violation, up to $25,000 per year. And criminal penalties apply as well – up to $50,000 in fines and a year in prison for knowingly disclosing PHI; up to $100,000 in fines and five years in prison if the disclosure is under false pretenses; and up to

$250,000 in fines and 10 years in prison if the disclosure is for commercial advantage.

GCD Note:
The HIPAA privacy rules cover insured plans as well, but compliance responsibilities often fall to health insurers in those cases. Therefore, this Memorandum focuses primarily on the impact these rules will have on self-insured plans and provides insights and guidance for navigating this unfamiliar terrain.

Plan documents

The HIPAA portability rules, which generally took effect in 1997, required plan amendments. However, those changes were not as broad and detailed as those required by the new privacy rules. Under the privacy rules, if you are an employer acting as a plan sponsor, you will have to certify to your own health plan that the plan documents have been amended and that, as the plan sponsor, you agree to abide by the new terms. Employers also will need to identify which employees are acting on behalf of the self-insured health plan and which are performing in other employer functions.

Specifically, the employer, as the plan sponsor, will need to amend plan documents to:

- Identify the permitted and required uses and disclosures of PHI.
- Require the plan sponsor certification mentioned above.
- Prohibit the plan sponsor from using or disclosing PHI other than as permitted or required by the plan documents or as required by law.
- Require any agents of the plan who receive PHI to abide by the privacy rules.
- Bar plan sponsors from using PHI for employment-related actions or in connection with any of its other benefit plans.
- Require the sponsor to report to the plan any improper use or disclosure.
- Give participants access to their PHI and enable them to amend it upon request (or be told why their requested amendment was denied).
- Provide participants, upon request, an accounting of all disclosures of their PHI.
- Make available to HHS its internal practices, books, and records relating to the use and disclosure of PHI.
- Require the sponsor, 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.
- Finally, to ensure separation between the health plan and the plan sponsor's other operations, the plan must: (i) describe which employees will have access to PHI; (ii) restrict this access to plan administration functions; and (iii) provide a way to resolve any violations of the privacy rules by these employees.

GCD Note:
The restriction on using PHI for other benefit plans could be significant for employers that, for example, use health plan data to evaluate or design disability plan benefits or that have integrated benefit plans. However, the regulations do permit the health plan to disclose PHI to the extent necessary to comply with workers compensation laws.

Of course, many of these plan document changes could entail substantial revisions to the way a plan currently maintains and protects health information. Currently, for example, health plans probably have no mechanism to provide (and may not even have the data to provide) a participant with a record and explanation of all the disclosures of his or her PHI (other than disclosures for treatment purposes).

Administrative services contracts

For many employers, negotiating detailed administrative services contracts has not been a high priority. But under the new privacy rules, a plan cannot disclose any PHI to any of these "business associates" – including claims processing and administration firms, utilization review and quality assurance firms, HMOs, managed care providers, billing companies, firms providing data analysis, aggregation, and administration, actuarial firms, legal and accounting firms, accreditation organizations, and firms providing financial services – without a written contract that:

- Establishes permitted and required uses and disclosures of PHI by the business associate.
- Permits the business associate to use or disclose PHI for proper management and administration.
- Permits the business associate to provide data aggregation services for the plan.

- Authorizes termination of the contract in case of a material breach.
- Prohibits the business associate from using or disclosing the PHI other than as stated in contract or as required by law.
- Requires the business associate to use appropriate safeguards.
- Requires the business associate to report to the plan any use or disclosure of PHI not provided for by its contract.
- Requires the business associate to ensure that any agents to whom it provides PHI abide by these privacy rules.
- Requires the business associate to give participants access to their PHI, and to amend it upon request (or explain why a requested amendment is denied).
- Requires the business associate to make available the information required to provide a participant an accounting of disclosures of his or her PHI (other than disclosures for treatment purposes).
- Requires the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure.
- Requires the business associate to destroy all copies of the PHI when the contract terminates or, if this is not feasible, to limit further uses and disclosures.

GCD Note:
Although these contract standards may seem burdensome, they may be a useful tool for employers in seeking better protection in services contracts.

Members of the health plan's workforce are not considered business associates when they perform these services. For example, claims administrators employed by the employer sponsoring the health plan will not be considered business associates.

Administrative policies and procedures

Beyond the plan documents and service contracts, the HIPAA privacy rules will require major revisions to the way an employer currently administers its self-insured health plan. Several of the key changes are highlighted below.

Privacy policy. A self-insured health plan will be required to adopt and communicate a detailed privacy policy to its participants. The policy must be written in plain English and must describe the uses and disclosures of PHI that are allowed for payment, treatment and health care operations, and describe the restrictions or limitations on uses or disclosures imposed by the HIPAA rules (or by more stringent state standard). The policy must also, among other things, describe a participant's right: (i) to request restrictions on the uses and disclosures of his or her PHI; (ii) to inspect, copy and request an amendment to his or her PHI; and (iii) receive an "accounting" of all uses and disclosures of his or her PHI (including the date, the name of the individual or entity who received the information, and a description of the PHI and the reason for its use or disclosure). The rules also govern how the policy can be modified and how participants are to be notified of any changes.

GCD Note:
Because HHS has no track record in regulating self-insured health plans, it is difficult to predict how aggressively it will enforce the rules.

Privacy official/training. A self-insured health plan will be required to designate a "privacy official" who will be responsible for developing and putting in place HIPAA-required policies and procedures. If the employer is a health care entity that already has a privacy official, that organization could use the same individual to act as the privacy official for its self-insured health plan.

An employer will also be required to provide appropriate training in handling PHI to each employee who performs health plan administration functions. This training must be provided initially by the time the HIPAA privacy rules take effect for the health plan (February 26, 2003, for plans generally or February 26, 2004, for plans with annual receipts under $5 million). An ongoing training program must be in place to address training of new hires or changes in privacy laws.

Participant complaints. Your health plan will also be required to provide a way for participants to file complaints about privacy policies and procedures or your compliance with these policies and procedures. All complaints received and their disposition, if any, must be documented. In addition, your plan may not intimidate, threaten, coerce, discriminate against, or take retaliatory action against: (i) individuals for participating in any process established under the HIPAA rules; or (ii) against individuals or others for filing a

complaint, testifying, assisting or participating in an investigation, compliance review, or proceeding, or opposing any act or practice prohibited by the HIPAA rules.

Preemption

The HIPAA privacy rules do not preempt state laws that are more stringent than the federal privacy protections. Many states currently have such laws or may enact them in response to the HIPAA privacy regulations. Because there may be different laws in different jurisdictions, employers with multistate operations should carefully monitor state privacy law developments.

GCD Note:
This may represent a major shift for self-insured health plans that were not ordinarily covered by state restrictions due to ERISA preemption.

Consent vs. authorization

The new HIPAA rules create a distinction between obtaining consent and authorization when getting permission to use or release PHI. For payment, treatment, and health care operations, a more generally worded and less restrictive form of permission may be required from a participant (consent). For all other uses or disclosures of PHI, a more comprehensive, specifically worded and restrictive form must be used to obtain permission for use or disclosure of PHI (authorization). Each of these is discussed in more detail below.

Consent. The new rules require that health care providers obtain an individual's consent prior to using or disclosing PHI to carry out treatment, payment or health care operations. A self-insured health plan may obtain consent, but is not required to do so. A plan may condition enrollment on obtaining consent.

Consent forms, which must be written in plain English and must be signed and dated, must also:

- Inform the participant that PHI may be used or disclosed for purposes of payment, treatment and health care operations.
- Refer the participant to a complete description of uses and disclosures in the health plan's general privacy notice.
- Indicate that the plan's privacy policy may be modified and how a revised copy of the policy can be obtained.
- State that the participant may request the health plan to restrict the use or disclosure of PHI and indicate that the health plan may refuse such request.
- State that the participant may revoke the consent unless the health plan has taken action in reliance upon that consent.

This consent requirement applies only to use and disclosures of PHI for payment, treatment and health care operations. The consent may be combined with other legal consents (such as a consent for assignment of benefits) provided that the consent is distinct from any other authorization and has a separate signature and date line.

Authorization. If PHI is going to be used or disclosed for any reasons other than payment, treatment, or health care operations (where no legal exceptions apply), the health plan must obtain authorization. For example, if the employer's disability plan requests information from the health plan about a participant, or if a participant asks that information be disclosed to an outside party, that disclosure would only be permitted if the health plan first obtained a written authorization from that participant. This is true even if the disability plan is only using the information to properly pay disability plan claims. The health plan may not condition treatment, payment, enrollment in a health plan or eligibility for benefits on the individual's signing of an authorization except in specific and limited circumstances.

GCD Note:
Rather than maintain authorizations, a health plan could consider using only health information that has gone through an elaborate process of "de-identification" to remove all potentially traceable pieces of information.

Similar to the consent form, an authorization form must meet certain criteria to be valid. Specifically, the form must: be written in plain English; describe the PHI to be used or disclosed; identify to whom the PHI will be disclosed; include an expiration date; include a right to revoke; and indicate that the PHI may be subject to redisclosure by the recipient where such disclosure might not be covered under the privacy statute and regulations.

* * *

Gardner, Carton & Douglas
HR Law Team

Marla B. Anderson manderson@gcd.com	(312) 245-8879
Mona L. Bentz mbentz@gcd.com	(312) 245-8530
Gregory K. Brown gkbrown@gcd.com	(312) 245-8864
Natalie Cadavid ncadavid@gcd.com	(312) 245-8724
Kathryn M. Clancy kclancy@gcd.com	(312) 245-8481
Lisa L. Collins lcollins@gcd.com	(312) 245-8467
Barbara A. Cronin bcronin@gcd.com	(312) 245-8746
Ralph E. DeJong rdejong@gcd.com	(312) 245-8466
Kimberly Frailey kfrailey@gcd.com	(312) 245-8477
Carol M. Hines chines@gcd.com	(312) 245-8484
Gary W. Howell ghowell@gcd.com	(312) 245-8763
Jeffrey M. Johns jjohns@gcd.com	(312) 245-8705
Frances P. LaFleur flafleur@gcd.com	(312) 245-8848
Howard J. Levine hlevine@gcd.com	(312) 245-8865
Joyce L. Meyer jmeyer@gcd.com	(312) 245-8757
Valerie L. Miller vmiller@gcd.com	(312) 245-8719
Sarah F. Rivera srivera@gcd.com	(312) 245-8760
Michael D. Rosenbaum mrosenbaum@gcd.com	(312) 245-8692
Mary K. Samsa msamsa@gcd.com	(312) 245-8868
Lori L. Shannon lshannon@gcd.com	(312) 245-8451
Edward Spacapan espacapan@gcd.com	(312) 245-8452
Timothy J. Stanton tstanton@gcd.com	(312) 245-8524
David L. Wolfe dwolfe@gcd.com	(312) 245-8438

Gardner, Carton & Douglas
HIPAA Task Force

Bernadette M. Broccolo, Chair bbroccolo@gcd.com	(312) 245-8454
Cathy Kiselyak Austin caustin@gcd.com	(312) 245-8429
Karen A. Erikson kerikson@gcd.com	(312) 245-8528
Jessica L. Eisenhaure jeisenhaure@gcd.com	(202) 408-7253
Anne Kurtz Flam aflam@gcd.com	(202) 408-7229
Edwin A. Getz egetz@gcd.com	(312) 245-8475
Gary W. Howell ghowell@gcd.com	(312) 245-8763
James M. Jacobson jjacobson@gcd.com	(202) 408-7191
James M Jorling jjorling@gcd.com	(202) 408-7131
Neela A. Paykel npaykel@gcd.com	(202) 408-7123
William H. Roach, Jr. wroach@gcd.com	(312) 245-8432
Colleen M. Roberts cmroberts@gcd.com	(312) 245-8534
Michael D. Rosenbaum mrosenbaum@gcd.com	(312) 245-8692
Timothy J. Stanton tstanton@gcd.com	(312) 245-8524
Priscilla A. ("Pam") Walter pwalter@gcd.com	(312) 245-8442
Elaine C. Zacharakis ezacharakis@gcd.com	(312) 245-8835

Gardner, Carton & Douglas

321 North Clark Street
Suite 3400
Chicago, Illinois 60610
(312) 644-3000

1301 K Street, N.W.
Suite 900, East Tower
Washington, D.C. 20005
(202) 408-7100