MILLER & CHEVALIER
CHARTERED

ERISA AND BENEFITS ALERT

October 31, 2002 **Volume 4 Issue 10**

TOP TWENTY HIPAA PRIVACY QUESTIONS ASKED BY EMPLOYERS WITH GROUP HEALTH PLANS

Employers are becoming aware that, because of their group health plans, they will have obligations under the new federal regulations governing the privacy of medical information.

To help you begin your compliance activities, this Alert covers the twenty questions we have most frequently been asked.

1. What is HIPAA? HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. Title I of HIPAA governs portability of health benefits, special enrollment, and non-discrimination rules. Title II, Subtitle F of HIPAA governs Administrative Simplification. The Administrative Simplification provisions are intended to make the health care information system more cost effective and efficient by requiring standardized electronic transmissions of certain claims-related information.

The Department of Health and Human Services has, so far, issued final regulations in two key areas governed by HIPAA: Privacy and Electronic Transactions. The compliance deadline for Electronic Transactions has passed and the deadline for Privacy is imminent. Numerous other related regulations will be issued or finalized in the coming months and years.

2. Do employers need to worry about complying with HIPAA? What if I'm a small employer? Almost every employer that offers health benefits to its employees will need to comply with HIPAA. The HIPAA Administrative Simplification regulations apply to employer group health plans. The only group health plans that will not be subject to HIPAA are those that have fewer than 50 participants (*i.e.*, covered employees) ***and*** are self-administered. There is no exception for small employers, but if your company has a "small health plan" as defined by HIPAA, it will have an extra year to comply.

3. I've heard that small health plans have more time to comply – does my group health plan fall in that category? If your group health plan is a "small health plan" under this guidance, then it has an extra year to comply with all of the HIPAA finalized regulations. That is, it has until October 16, 2003, to comply with the HIPAA Electronic Transactions regulations and until April 14, 2004, to comply with the HIPAA Privacy regulations.

A small health plan is defined as a plan with annual receipts of $5 million or less. Guidance from the HIPAA regulators advises that a fully-insured plan should use total premiums paid for health benefits and a self-insured plan should use the total amount paid for health care claims. Stop-loss premiums should not be included. A plan that is partly insured and partly self-insured should combine the measures. The applicable period is the last full fiscal year. There is a different measure for health plans that file tax returns.

4. Is the $5 million threshold for "small health plans" applied to each of my company's group health plans separately? The regulations provide no guidance on this point. It appears that the $5 million threshold applies to each separate group health plan. The regulations also provide no guidance on determining the number of group health plans. One approach might be to use the number of IRS Forms 5500 your company files as a guide. An approach for

non-ERISA plans might be to consider how the plans are disclosed to participants.

5. My group health plan does not transmit any information electronically. Are we exempt from the HIPAA Privacy and Electronic Transactions regulations? No. Group health plans are covered entities whether or not they transmit information electronically. Providers, such as doctors, nurses, on-site clinics, etc., *do* avoid coverage under these regulations if they do not transmit electronically. Again, this exception does not apply to group health plans.

6. Does it matter whether my company's group health plan is fully insured or self-funded? It matters a lot. There can be a significant difference. In general, a fully-insured group health plan that receives only limited information about its participants and beneficiaries will have a lighter compliance burden. For most such fully-insured group health plans, it may be that their insurance issuers or HMOs will bear the brunt of the compliance burden.

A self-funded group health plan, on the other hand, is presumed to receive information about its participants and beneficiaries and will have a significant compliance burden. For example, self-funded group health plans that retain responsibility for final review of contested benefit claims, and therefore receive this kind of information, will have to comply with all of the requirements of the regulations.

7. What are my company's obligations under HIPAA? You company's HIPAA obligations will vary depending on whether its group health plan(s) is fully-insured or self-funded, on the type of identifiable health information it receives about employees and their families, and on whether it provides other employee health services (such as on-site clinics) that are covered by HIPAA. If your company is covered indirectly as the sponsor of a group health plan, or directly as a health care provider, or both, it may be required to:

- Follow detailed rules about how it uses internally or discloses externally employee and family health information;
- Implement new federal rules granting rights to employees and their covered family members relating to information in group health plan records or provider records;
- Implement numerous other administrative requirements such as written policies and procedures, workforce training, designating a privacy official, and distributing a notice of its privacy practices, to name a few; and
- Comply with HIPAA's rules governing the eight specific transactions that are required to be transmitted electronically in a standardized format.

8. Will I still be able to help my employees with their benefit claims? Yes, but this is a complicated issue. An employer generally will be able to help its employees with their benefit claims. It is likely, however, that the employee will need to provide an authorization to the insurer, HMO, or third-party administrator before those entities will share information needed to resolve the benefits issue. You might consider requesting participants to sign authorizations for this purpose when they enroll in your group health plan. Be aware, however, that you cannot condition enrollment on receiving such an authorization. Also, the authorization must describe the purpose of the requested use or disclosure (that is, it cannot be a blanket authorization for the release of health information for any and all purposes). The authorization should also include an expiration event such as "end of employment." Be sure and check the Privacy regulations for more information about the content and use of authorizations.

Note that some employers may be able to avoid the authorization requirement, provided HIPAA otherwise requires them to amend their plan documents and those amendments specifically permit the disclosures necessary for this type of employee assistance.

9. Do I need to change the way I handle medical information relating to pre-employment physicals, fitness-for-duty, drug-free workplace tests, etc.? HIPAA does not affect these types of employment-related medical tests so long as the employer does not obtain any such information from its group health plan or from employees who are covered providers. It is more likely that the information an employer receives relating to these tests is from outside physicians. The employer does not have any HIPAA concerns with this information because it does not come from the

employer's group health plan or from an employee covered provider. The outside physician is likely to be a covered provider under HIPAA and may require the employee to provide a HIPAA authorization before he or she will release the health information to the employer. An employer may require such authorizations as a condition of employment.

10. How does HIPAA affect medical information relating to workers' compensation cases? HIPAA has a special rule permitting an employer to release information from its group health plan for purposes of complying with state and federal workers' compensation laws. The disclosure must only include that information that is "authorized by" and "necessary to comply with" the relevant law. This information may be less than the group health plan is currently providing.

11. Is there a model privacy policy available? HIPAA requires numerous privacy policies and procedures to be adopted and implemented. These policies and procedures must be summarized in a required notice. Thus, there is no single "privacy policy," but there is a required summary notice. The final Privacy regulations do not include model language for these requirements. There are commercially-available compliance products to assist you in drafting your policies and procedures and notices, including one prepared by Miller & Chevalier. For more information, please see www.millerchevalier.com/kit.asp.

12. I've heard we need to revise our service provider contracts because of HIPAA. Is that true? Under the HIPAA Privacy regulations, a service provider that creates or receives employee/family health information must contractually agree to protect that information to the same extent that the group health plan is required to protect it. Such a service provider is called a "business associate."

Generally, a self-insured group health plan will need to include special provisions in each contract with a service provider that is considered to be a business associate. This includes, for example, contracts with its third-party administrator(s). A fully-insured group health plan is not required to have a business associate contract with its insurers and/or HMOs. A recent amendment to the Privacy regulations provides for an extension of up to one year for amending written service provider contracts to include business associate provisions. This extension applies only to written contracts that were in existence on October 15, 2002, and that are not amended before April 14, 2004. This extension is helpful, but does not provide complete relief from the business associate requirements during the extension period.

13. Does HIPAA affect my compliance with the ADA and FMLA? HIPAA affects compliance with the ADA or FMLA only if an employer obtains information from its group health plan or from an employee covered provider to comply with those laws. It is more likely that the information an employer receives relating to ADA and FMLA compliance is from outside physicians or directly from its affected employees (such as to establish the need for a reasonable accommodation). The employer does not have any HIPAA concerns with this information because it does not come from the employer's group health plan or from an employee covered provider. Other laws may provide confidentiality protections, of course. The outside physician is likely to be a covered provider under HIPAA, and may require the employee to provide a HIPAA authorization before he or she will release the health information to the employer. Most employees seeking to exercise their ADA or FMLA rights will likely provide such an authorization.

14. Is our health FSA covered by HIPAA? What if our other health benefits are fully insured? Yes. An FSA is a group health plan under HIPAA and has not been given an exemption under Title II. Note that even if your other health benefits are fully-insured, FSAs are generally self-insured. Self-insured group health plans generally have a heavier HIPAA compliance burden. We understand that the HIPAA regulators are reviewing the status of FSAs and may issue guidance at some time in the future. If your FSA is the only self-funded group health plan in your benefits package, and if it would qualify as a "small health plan" if you treated it separately, you might wish to do so (*i.e.*, by treating it as a separate plan for ERISA reporting and disclosure purposes). This would allow you to take advantage of the later compliance date for small group health plans and also any helpful guidance that the HIPAA regulators may issue.

15. My company has an on-site clinic. Do we need to be concerned about HIPAA? Yes, your on-site clinic might be a covered provider. HIPAA applies to all providers electronically transmitting any one of the eight transactions that have been standardized. If your onsite clinic conducts any such transactions electronically, then it will need to comply with HIPAA's Electronic Transactions regulations and its Privacy regulations.

16. Do I need to comply with any state privacy laws? Possibly. A state privacy law that provides more privacy protections or greater individual rights than provided by the federal HIPAA regime will apply, unless that law is otherwise preempted by a different federal law, such as ERISA.

17. Are there special rules or exceptions for non-profit employers? No. Non-profit organizations are treated like any other employer.

18. Are there special rules or exceptions for government employers? Government employers must comply with the HIPAA regulations. Those regulations, do, however, have some special rules that recognize the inability of government entities to enter into contracts (for instance, for business associate contracting purposes). Instead, government employers may enter into "memoranda of understanding" (MOUs) with their business associates.

19. Are there penalties for not complying with the HIPAA requirements? Yes. There are both civil fines and criminal penalties, including imprisonment. The civil fines are $100 per violation, up to $25,000 a year for each standard violated. Criminal penalties for knowing misuse of protected health information may be as high as $50,000 and one year of imprisonment. There are higher criminal penalties for false pretenses and for intent to sell information.

20. Where can I obtain a copy of the HIPAA regulations? The Privacy regulations are available at www.hhs.gov/ocr/hipaa/finalreg.html. For information about the other final and proposed Administrative Simplification regulations, see aspe.hhs.gov/admnsimp/.

Will Your Group Health Plan Be Ready By April 14, 2003?

Self-funded plans generally must meet all the obligations of the Privacy rules. To help employers with self-funded group health plans comply, our ERISA and HIPAA attorneys are providing a Privacy Compliance Kit for Self-Funded Group Health Plans. The kit combines (1) on-site training and evaluation, (2) tailored model documents and a tailored implementation analysis, and (3) follow-up support, at a low fixed cost. Please see www.millerchevalier.com/kit.asp for more information, including a sample chapter.

Questions? Contact us as indicated below or at privacy@milchev.com.

Miller & Chevalier Employee Benefits Practice Group

C. Frederick Oliphant
foliphant@milchev.com
(202) 626-5834

Anthony F. Shelley
ashelley@milchev.com
(202) 626-5924

Serena G. Simons
ssimons@milchev.com
(202) 626-5867

Lisa T. Murphy
lmurphy@milchev.com
(202) 626-5948

Maria O'Toole Jones
mjones@milchev.com
(202) 626-6037

Jeanette Dayan
jdayan@milchev.com
(202) 626-6037

Adam B. Walker
awalker@milchev.com
(202) 626-5956

www.millerchevalier.com