



WHAT EMPLOYERS NEED TO KNOW (AND DO) ABOUT THE NEW HIPAA PRIVACY REGULATIONS

Presented by Eric N. Athey

I. INTRODUCTION

With the country focused on our conflict overseas and a Republican administration in the White House, employers may be justified in expecting little by way of new employment regulations over the next few years. However, although the Bush administration wasted no time in derailing the now infamous OSHA ergonomics regulations in early 2001, the administration declined to take the same approach toward medical privacy regulations that were initially proposed in November 1999 by Donna Shalala, Secretary of Health and Human Services ("HHS") under the Clinton administration. These regulations, which were proposed in accordance with the Health Insurance Portability and Accountability Act of 1998 ("HIPAA") are now scheduled to become effective on ***April 14, 2003*** (2004 for health plans with annual receipts of \$5 million or less).

The final medical privacy regulations were published in the Federal Register on December 20, 2000. The regulations themselves are lengthy and, in many areas, likely to confuse anyone who is not thoroughly familiar with the terminology utilized by HHS in connection with HIPAA. A copy of the actual regulations is available on-line at **<http://aspe.hhs.gov/admsimp>**. A fact sheet concerning the regulations may also be accessed at **www.hhs.gov/news/press/2000pres/00fsprivacy.html**. Additional guidance regarding the regulation is also available on HHS's website at **www.hhs.gov/ocr/hipaa**.

In sum, the new regulations will dramatically affect the manner in which medical information may be shared among interested parties. The regulations impose strenuous requirements on certain entities that are likely to deal with such information on a routine basis, such as health care providers, insurers and self-insured health plans. For the majority of employers, the regulations do not require much by way of immediate action; however, they will dramatically affect the manner in which employers can access and use medical information. This outline summarizes the impact that the regulations will have on employers in their capacity as employers. The intent is to assist employers in focusing on what they need to do in order to comply; however, this outline is not an exhaustive recitation of all compliance requirements. Likewise, special requirements which apply to health care providers, insurers and other covered entities are not addressed here except to the extent relevant to the general discussion.

II. THE PRIVACY RULE IN A NUTSHELL

Reduced to its most basic form, the "rule" imposed by the new regulations is as follows:

"Covered entities" may not use or disclose "**protected health information**" ("PHI") except as **authorized** by the individual who is the subject of the information, or as explicitly **required or permitted** by the regulation. Even when the use or disclosure of PHI is permitted, in most cases, the regulations require that only the "**minimum necessary**" amount of information be given to accomplish the intended purpose of the use, disclosure or request.

Simple as this rule may seem, the regulations are lengthy and, at points, difficult to understand. To begin to understand the impact of the regulations on employers, one must first examine the key definitions in the regulations.

III. KEY DEFINITIONS

Covered Entities. The regulations broadly define "covered entities" to include:

A health plan;

A health care clearinghouse; and

A health care provider who transmits health information in electronic form in connection with transactions (i.e. exchanges of information) covered by HIPAA's administrative requirements.

Covered entities do **NOT** generally include:

Employers;

Unions;

Plan sponsors;

Life, disability and workers' compensation insurers.

NOTE: As discussed below, employers may become covered through their operation of a self-insured health plan or in-house health facilities.

Protected Health Information ("PHI"). PHI is individually identifiable health information that is transmitted or maintained by electronic media or is transmitted or **maintained in any other form or medium**. To constitute "health information", information must relate to the **past, present or future physical or mental health condition of an individual** or relate to the provision of health care or the payment for health care provided to an individual. To constitute individually identifiable health information, information must either **identify the subject individual** or create a **reasonable basis for believing** that the subject would be identified. The regulations apply to all protected health information maintained, used or disclosed by a covered entity, regardless of the form of the information (e.g. written, oral or electronic). The information remains protected for the life of the individual and for as long as a covered entity maintains the information.

Consent. The regulations provide that a subject individual must grant his or her broad general permission, or "consent," to a health care provider to disclose the individual's PHI for purposes of **treatment, payment or health care operations ("TPO")**. However, a health care provider generally may not disclose PHI to a non-covered entity or non-business partner without a more specific "authorization." Consent is a less onerous requirement than authorization because: (1) it need only be provided once until revoked; (2) it may be granted via a brief, written consent form. Signed consents must be maintained by a covered entity for a minimum of six years. **Health plans and clearinghouses** may use and disclose PHI for TPO without obtaining consent; however, disclosure to non-covered entities must generally only be with specific authorization unless an exception applies. (See attached HHS Guidance).

Authorization. If an "authorization" is required, it must be **written** and **specifically describe** the information at issue; **name the person(s) authorized** to make the disclosure; **name the person(s) to whom the disclosure may be made**; contain an **expiration date**; state that the individual **may revoke** the authorization in writing and describe **how to do so**; and be **signed by the subject individual**. In addition, if the disclosure will be to a non-covered entity, the authorization must clearly state that the individual understands **the disclosure removes any privacy protections** that had attached to the PHI. If a covered entity initiates the request for an authorization, additional requirements apply, the most troublesome of which is that treatment, payment, **enrollment in a health plan, or eligibility for benefits cannot be conditioned on the individual's authorization.**

IV. IS YOUR ORGANIZATION A COVERED ENTITY?

Entities which are not in the health care or health insurance industry may quickly assume that they are not "covered entities" under the regulations. However, the definition of "covered entity" may be broader than one might initially suspect. Employers in other industries may find themselves to be "covered entities", or "**hybrid entities**", due to their sponsoring a self-insured group health plan or their operation of a medical department. In addition, by offering health insurance in any form, an employer may now be affected by the new limitations placed on their insurers regarding the disclosure of pertinent medical information.

A. Compliance Issues Arising From Your Health Plan.

Covered entities include "**health plans.**" A "health plan" is broadly defined in the regulations to mean an individual or group plan that provides, or pays the cost of, medical care. The term includes:

Virtually all group health plans (insured or self-insured) **covered by ERISA** (i.e. plans with 50 or more participants or any plans administered by other entities);

Government and church plans;

Health insurance issuers;

HMOs;

Medicare; and
Flexible spending accounts.

Determining Whether Your Plan is Fully Insured or Self-Insured. The extent of the impact of the new regulations on an employer's health plan will largely depend on whether the plan is **insured** (e.g. an insurer provides coverage through a group agreement with the employer) or **self-insured** (e.g. the employer provides coverage through a trust that is administered by the employer or a third party administrator). In most cases, making this determination will be simple. However, as health care costs escalate, employers and their insurers are increasingly "blurring the lines" between insured and self-insured status. Issues that should be considered in determining whether a plan is fully insured include: Is there **risk sharing** between the employer and the plan? Who ultimately makes **coverage determinations**? How is the plan compensated? Depending on the answers to these questions, it may not be easy to classify your plan's status. As an employer's involvement with its health plan increases along these lines, so does the risk that its plan will be considered self-insured. This is an issue that will hopefully be the subject of further guidance from regulators and the courts.

Insured Plans. Since most employers and other entities that sponsor insured group health plans are not covered entities, the general rule of limited disclosure would typically require an insured plan to obtain individual authorization before releasing PHI to the plan sponsor. However, recognizing that this could be unduly burdensome, the drafters of the regulations allowed for an **exception** to the "authorization" requirement in this instance, provided certain conditions are met:

Plan documents must be amended to identify which employee(s) of the plan sponsor will have access to the PHI and the purposes for which it will be used;

If the designated recipients perform other non-plan functions for their employer, **"firewalls"** must be established to ensure that the designated recipients do not use PHI for non-plan purposes (e.g. disciplinary issues);

An effective **mechanism** must be established **for resolving compliance issues**; and

The plan **must certify that the necessary amendments have been made** and PHI may only be released to the plan sponsor once the group health plan receives this certification;

The **certification** must assure that: the plan sponsor will not use or disclose PHI except as permitted by the plan document or as required by law; any agents or subcontractors (e.g. consultants, attorneys, third party administrators) to whom the plan sponsor may provide PHI will abide by the same restrictions; the PHI will not be used for employment-related actions or in connection with any other non-group health benefit plan offered by the sponsor; to report to the group health plan any use or disclosure which is inconsistent with the permitted uses; to make the PHI available as required by the regulation (mainly to the subject individual); to make

its books, records and practices available to HHS for audit purposes; to return or destroy all PHI when no longer needed; to ensure confidentiality in all other respects.

Of course, if a group health plan merely provides "**de-identified**" health information to a plan sponsor, these requirements would not apply. "De-identified information" is PHI from which **all identifying data that could enable someone to discern the subject has been removed**. Likewise non-health information, such as **enrollment forms** that do not include medical history, etc. does not constitute PHI.

Self-Insured Plans. When an employer sponsors its own self-insured group health plan, **the plan is, in its own right, a covered entity** and subject to all of the limitations that attach to this status. In sum, an employer must ensure that its health plan component meets all requirements that apply to covered entities and not disclose PHI to any other component of the employer, except as permitted by the HIPAA regulations. Any employee involved with the plan's administration who performs other non-plan functions for the employer may not disclose PHI except as permitted by the regulations. Some of the additional specific requirements for self-insured plans include:

Disclosures of PHI must be limited to situations involving **payment, treatment, or operation of the plan;**

For payment and operation purposes, the **minimum necessary rule** applies;

The plan must **obtain participant consents and authorizations as required** of other covered entities;

The plan must provide **notice of its policies** regarding PHI privacy;

Subject individuals must be given (i) **access** to their PHI; (ii) **permission to correct** inaccurate information; and (iii) **an accounting** of all disclosures of PHI that were not for payment, treatment or operation of the plan;

The plan must appoint a **privacy officer** and privacy contact person;

The plan must **adopt policies for managing PHI** and safeguarding privacy;

Providing **training to all employees** with respect to its privacy policies;
The plan must provide a **mechanism for individuals to challenge** or dispute the use of PHI and sanctions for violators of established policies;

The plan (or any other covered entity) **may not require individuals to waive their privacy rights** under the regulation as a condition of enrolling in the health plan, eligibility for benefits, treatment, or payment; and

The plan must **maintain documentation of its policies** and procedures for

complying with the regulations.

Third Party Administrators and Other "Business Associates." As a general matter, a self-insured health plan or clearinghouse, may disclose PHI without general consent from the subject individual for purposes of "treatment, payment or health care operations" (TPO). The regulations recognize that there are a wide variety of non-covered entities that a covered entity may need to share PHI with in carrying out functions related to TPO. This group of entities is generally referred to in the regulations as "**business associates.**"

In the case of a self-insured health plan, likely business associates include: **third party administrators, counsel, actuaries, accountants, consultants and billing and other financial services firms.** Generally speaking, a covered entity may only share PHI with business associates in accordance with a contract that limits the use and disclosure of PHI under the same restrictions that apply to the covered entity. The **business associate contract** must:

- set out the **permitted and required uses** of PHI;
- provide that the business associate will (i) **not use PHI except as permitted** by the regulation; (ii) use **appropriate safeguards**; (iii) **report any inappropriate usage**; (iv) ensure that its employees and agents **agree to the same restrictions**; (v) **permit HHS to audit their books, practices and records** relating to PHI.

If the covered entity and business associate are both **government entities**, the contract requirement may be satisfied through a **memorandum of understanding.**

In addition to signing the required contract, a business associate must, in some cases, appoint a **privacy officer**, undertake privacy **training** and other steps similar to those listed above for self-insured plans.

B. Compliance Issues Arising From Your Medical Department.

Employers that have in-house medical departments or on-site health clinics may qualify as "**hybrid entities**" (i.e. partially covered entities) under the new regulations **if** the department or clinic **utilizes electronic communications technology** to do one of the following: (i) transmit or receive health care claims; (ii) transmit or receive health care payment or remittance advice; (iii) transmit or receive health care claim status; (iv) determine eligibility for a health plan; (v) transmit or receive referral certification and authorization; (vi) transmit or receive the first report of injury; or (vii) transmit or receive health claims attachments.

Even if the clinic or department does not perform any of these functions, compliance with the regulation may make sense since HIPAA's privacy requirements may very well become the expected "**standard of care**" in lawsuits alleging invasion of privacy arising from unauthorized disclosure of health information.

Assuming your in-house clinic or health department converts your organization into a hybrid entity, many of the same rules outlined above for covered entities such as self-insured health plans will apply to the covered component of your operation.

VI. SELF-ASSESSMENT AND ACTION PLAN FOR HUMAN RESOURCES

HIPAA compliance initiatives can be challenging for employers because effective initiatives must combine skills and knowledge that are typically spread among departments. An effective compliance initiative may involve auditing functions traditionally reserved to a company's finance department; training and policy development functions traditionally reserved to human resources; risk assessment traditionally reserved to a risk manager or safety officer and medical review typically reserved for a plan administrator or plant nurse. The employer that can effectively pool its resources and apply them in a cost-effective manner should find compliance manageable.

Any compliance initiative must begin with a self-assessment. Where does your organization fit under the regulations and how do you comply with the applicable requirements (or, for most employers, how do you continue to obtain necessary information despite restrictions imposed on other covered entities)? From an H.R. perspective, a self-assessment should, at a minimum, include some analysis of the following points:

Attendance and Leave of Absence Policies. Human resources departments are perhaps most likely to obtain PHI in connection with their administration of attendance and leave of absence policies. A doctor's note, a medical certification or recertification and a return to work note would all presumably qualify as PHI since they either relate to the past, present or future physical or mental health or condition of an individual or the provision of care to an individual.

As noted above, an employer is generally not a "covered entity" and, therefore, a health care provider would typically need specific authorization from an individual in order to release such information to an employer. This additional "hurdle" for the administration of attendance and leave policies could complicate their enforcement. Can an employer use PHI against an employee if it was not properly released by a covered entity? Does the specific authorization requirement permit employees to delay release of information until they find a doctor who says what they want? How much time must an employee be given to provide the necessary authorizations?

Employers may be able to avoid some of the additional burdens posed by HIPAA by **merely requiring that employees produce the medical documentation** necessary to substantiate absences or sustained leaves of absence. The regulations very clearly require covered entities to release PHI to subject individuals upon request. By requiring that the employee serve as the conduit through which all PHI flows to an employer, employers may be able to avoid having to obtain specific authorization in most cases.

Of course, there will be situations where an employer needs or prefers to obtain medical information directly from a covered entity. For example, in cases where an injured employee is

incapacitated and cannot produce the necessary FMLA certification, an employer may opt to obtain a specific authorization permitting the covered entity to provide the information to the employer directly. Likewise, in cases where an employee is suspected of **falsifying** medical information, an employer may prefer to receive all information directly from covered entities pursuant to an authorization.

The challenge for human resources departments will be to review all policies and related forms which may periodically intersect with PHI and ensure that they reserve all necessary rights for the employer to require an employee to either provide the necessary authorizations or the PHI itself.

It is expected that the U.S. Department of Labor will be revising its sample FMLA certification form to incorporate HIPAA privacy concepts.

NOTE: FMLA regulations limit the extent of information that an employer may require in connection with a leave request and the extent of communications between an employer and an employee's health care provider (i.e. to clarify doctor's statements). Interestingly, FMLA allows employers to obtain other medical opinions when they have **reason to doubt** the validity of an employee's leave certification. However, an employer may need to obtain a HIPAA authorization in order to obtain the text of the second opinion.

Light Duty and Other Reasonable Accommodations. The Americans with Disabilities Act (ADA) permits employers to require medical documentation to substantiate the need for light duty or other reasonable accommodations. A covered entity will generally only be permitted to release this information directly to the employer with specific authorization from the subject individual. This formality might be avoided if an employee is required to obtain the documentation himself and provide it to the employer. However, as described above, there will likely be situations where the employer would want to obtain the information directly from the covered entity. Once again, policies and related forms should be reviewed and revised to ensure that the employer retains all rights to obtain the necessary information either directly from the employee and/or to require specific authorization to obtain it from a covered entity.

NOTE: The ADA already prohibits employers from making medical inquiries or requiring medical examinations unless "**job-related and consistent with business necessity.**" Once such information is obtained, the ADA requires that it be treated as **confidential** information and **separated** from general personnel information. The same is true for independent medical examinations (IME) that may be required of an employee in connection with various types of benefit claims and employment litigation.

OSHA Compliance. Certain OSHA regulations and state laws require employers to conduct **medical testing and monitoring** (e.g. tuberculosis testing; audiometric testing). The resulting PHI may be disclosed to the employer if the information is needed by the employer to comply with OSHA requirements or similar legal requirements. However, once again, related policies should be reviewed in light of HIPAA and to ensure that the employer retains all necessary rights to comply with its testing obligations.

Substance Abuse Testing. Companies that are solely engaged in the practice of conducting substance abuse testing at employer worksites may not be "covered entities" under the regulations. However, such companies typically utilize a laboratory with a medical review officer (MRO); such labs would, in most cases, presumably qualify as covered entities. For this reason, employers should again revise existing policies to incorporate the specific authorization requirement as necessary.

Employment Litigation and Subpoenas. Employers may need to obtain PHI regarding an individual in order to defend a claim of disability discrimination or similar charges. Likewise, employers periodically receive subpoenas to release file information that may include PHI (e.g. prior doctor's notes, medical leave certifications, etc.). Employers and covered entities may release PHI as expressly required by a **court order** or in response to a **subpoena** if they receive satisfactory assurance from the party seeking the information that (1) **reasonable efforts** have been made to ensure that the individual who is the subject of the PHI that has been requested has been **given notice** of the request; or (2) reasonable efforts have been made by the party to secure a **qualified protective order** that meets the requirements of the Privacy Rule.

Workers' Compensation. Workers' compensation insurers **are not** covered entities. Since they are not covered entities, they are only permitted to obtain PHI from covered entities with individual authorization. However, the regulations permit covered entities to release PHI **as required by law**. It remains to be seen how Pennsylvania's workers' compensation statutes will be interpreted in this regard. Once again, employers should be sure to review all related policies, procedures and forms to ensure that the employer retains all rights to obtain the necessary information either directly from the employee and/or to require specific authorization to obtain it from a covered entity.

Other Items for H.R.'s "HIPAA To Do List."

- Review H.R. considerations listed above; implement necessary policy changes;
- Determine whether any of the employer's health benefits are self-insured (including carve outs, mental health, vision and dental) Self-insured employers must take all compliance steps listed above and as required of covered entities (e.g. appointing privacy official; preparing business associate contracts; employee training and notices, etc.);
- Ensure current record retention and confidentiality policies comply with HIPAA;
- Conduct employer-wide audit to determine sources, uses, retention and disclosures of PHI;
- Amend group health plan documents to permit the necessary level of information sharing;

- Implement operational changes to comply with necessary plan amendments (e.g. "firewall" requirements);
- Consider whether you must require business associate contracts or whether such contracts will be required of your business;
- Evaluate whether employee training on HIPAA requirements is required or advisable;
- Evaluate whether there are ways to reduce your compliance responsibilities by restructuring or outsourcing various functions.

VII. HIPAA ENFORCEMENT

Under the new privacy regulations, the Secretary of HHS can impose civil monetary penalties against covered entities for up to \$25,000 per standard per year. Criminal penalties may also be imposed in certain cases which could result in penalties of up to \$250,000 and/or imprisonment of up to 10 years.

Private suits are not authorized by the regulations. However, covered entities could certainly sue business associates for damages incurred by them as a result of unauthorized disclosure of PHI. Likewise, individuals are likely to cite HIPAA regulations as the applicable "standard of care" in tort suits alleging invasion of privacy involving unauthorized release of medical information.