HIPAA LEGAL UPDATE

by

Scott Warrick, JD, MLHR, CEQC, SPHR

Scott Warrick's Consulting & Employment Law Services
(614) 367-0842: Office (614) 738-8317: Cell

www.scottwarrick.com

I. HIPAA PRIVACY REGULATIONS

A. Coverage

As of April 14, 2003, the "Privacy Requirements" of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) became effective for many employers. (HIPAA's various standards appear at 45 CFR parts 160 and 164.) While it is true that HIPAA's Privacy Rule does not directly cover employers, an employer who sponsors a group health plan or who has such privacy information regarding its employees in its possession will be affected nonetheless.

B. Which Plans Are Covered And When Are They Covered?

Almost all group health plans are covered. (The only plans that are exempt are those self-insured plans with fewer than 50 participants and are administered **exclusively** by the employer. **ALL** fully insured plans with $5,000,000.00 or more in receipts each year are covered.)

HIPAA's definition of a health plan is broad enough to encompass not only medical plans, but also other benefit plans such as dental, vision, prescription drug plans, employee assistance plans (EAPs) and flexible spending accounts. Unless the plan sponsor chooses to designate them collectively as an "**Organized Health Care Arrangement**," each plan must stand on its own with respect to meeting its HIPAA obligations.

"Small plans" automatically have an extra year to comply with the April 14, 2003 Privacy Rule deadline. (**Until April 14, 2004**) A small plan is one that has annual receipts of $5 million or less. However, small plans should not wait too long before starting their "trek" to compliance. As anyone can see form these materials, complying with HIPAA's Privacy Requirements is not small task … which is why the extension was given.

C. Personal Health Information Defined

Personal Health Information ("PHI") includes medical or mental records or other data that contains any type of health information that identifies the individual that is either stored or transmitted by the organization in any form, such as electrical, paper or oral transmission. Therefore, in order to be classified as PHI, the individual's name need not be included in the information. If a person's Social Security Number or birth date is included with the health information, then the information qualifies as PHI information under HIPAA.

D. Who and What Is Covered By HIPAA?

There are basically three categories of HIPAA coverage:

1. **Health Care Providers**

2. **Health Care Plans**

3. **Health Care Billing Providers**

Therefore, in a **VERY** technical sense, employers are not really covered by HIPAA … their health plans are covered. However, since many employers offer health care coverage to their employees, the employer **may** be required to comply with HIPAA if the employer receives "Personal Health Information" ("PHI") regarding their employees under this plan.

If an employer **NEVER** receives **ANY** claim information that identifies any of the participants' identities in any way, then the employer is not covered under HIPAA.

However, if the employer receives information that identifies the participants in **ANY WAY** way, such as by birth date, then this will be classified as PHI under HIPAA. This often happens at renewal. Employers often receive information regarding its most expensive claims for the year and the claimant is identified by birth date.

Therefore, if an employer receives **ANY** PHI information, then the employer must comply with HIPAA.

Additionally, if an employer has on-site medical services, such as with a company nurse, the company is covered by HIPAA as a provider.

E. Where Does HIPAA Hide?

HIPAA tends to "hide" in a few different areas for human resource professionals.

1. Health Insurance Renewal

HIPAA usually bites employers at renewal time. At renewal, in order to obtain other quotes, employers will receive large claims experience information. This information usually identifies employees, or their dependents, by their social security number, birthday, or by some other code. The person's medical claim information is included. As a result, the employer has just received PHI. The employer could easily be covered by HIPAA. Further, once an employer receives this PHI information for renewal, the employer will more than likely distribute this PHI information to other carriers. **THAT** distribution is covered by HIPAA. This means Business Associate Agreements must be secured before this information is distributed.

2. Section 125 Unreimbursed Medical Information

Many employers have Section 125C Unreimbursed Medical Accounts for their employees … and many employers administer these plans themselves. (A Section 125C Unreimbursed Medical Account is a welfare benefit plan that allows employees to pay for their unreimbursed medical, dental and vision expenses with pre-tax dollars.) Since the IRS classifies these plans as health plans, if an employer receives this information, that employer is covered by HIPAA. (It is also important for employers to realize that in many instances, their Section 125C Unreimbursed Medical Accounts are covered by COBRA as well.)

F. What About Substance Abuse Testing and Fit-For-Duty Examinations?

Even if an employer does not receive PHI in relation to its health plan, many employers have adopted Substance Abuse Testing Programs (i.e., Drug and alcohol tests). The substance testing performed under these programs is also covered by HIPAA <u>if the testing is paid through the company's insurance provider</u>, so the employer must have certain forms in place ready to use in order to comply. (i.e., Business Associate Agreements, Authorization and Release Agreements, etc.)

Also, when an employer questions the ability of an employee to perform his/her essential functions, the employer may want to have the employee undergo a medical examination. These medical examinations are covered by HIPAA as well if the testing is paid through the company's insurance provider, so HIPAA requirements must be met. Therefore, again, the employer must have certain forms in place ready to use in order to comply. (i.e., Business Associate Agreements, Authorization and Release Agreements, etc.)

Again, even if the employer is not covered by HIPAA, the **PROVIDER** is covered (i.e., Testing facility, physician's office, etc.). Therefore, employers should at a minimum have their HIPAA Authorization and Release Forms in place. If not, then the testing facility or physician's office cannot legally release this information.

G. What Are "Receipts"?

Fully insured plans should use the amount of **total premiums paid for health insurance benefits during the plan's last fiscal year**.

Self-insured plans should use the **total amount paid for health care claims by the employer, plan sponsor or benefit fund on behalf of the plan during the last full fiscal year.**

Plans that provide benefits through a mix of insurance and self-insurance should combine these measures to determine their total annual receipts.

If the plan's annual receipts are $5 million or less, then the plan automatically qualifies for one-year extensions of both deadlines described above.

H. Complying With The Privacy Rule By Identifying Data

Regardless of which category a plan fits into, HIPAA's Privacy Rule requirements should be considered.

The Privacy Rule imposes numerous requirements that safeguard **individually identifiable health information and provides employees with notices of their privacy rights and access to their records**. It also requires establishment of additional physical and procedural safeguards. Many of these requirements vary, depending upon the kind of information employers receive, who receives it, how it is used and whether your plan is insured or self-insured.

To begin preparing to meet these requirements, human resource professionals should conduct an assessment of exactly what areas of their organization handle **any type of** individually identifiable health information. If the organization operates an on-site medical clinic, the organization's obligations will be greater than those imposed upon employers who do not operate such services, at least for that portion of the organization.

Human resource professionals should determine:

1. What types of individually identifiable health information you currently receive;

2. Who sees it;

3. How they use it;

4. Where it is retained; and

5. Whether such access and use is necessary to accomplish the organization's purposes.

This assessment is where human resources should begin establishing its HIPAA compliance plan.

I. Authorization and Disclosure Agreement for Specific Instances *(Used By Employers Covered By HIPAA And NOT Covered By HIPAA)*

Other areas of the law affect the HIPAA Privacy Requirements. Specifically, in order to obtain information from health care providers so the organization might determine an employee's ability to return to work, what accommodations he/she may need to return to work under the ADA, his/her coverage under the ADA or FMLA, an Authorization and Disclosure form will be needed. This form should be made part of your FMLA/ADA documentation packet.

Also, since either an employer's "Substance Abuse Testing Program" and "Fit-To-Return-To-Work" medical examinations may be covered under HIPAA, if the employer's insurance plan pays for the test, or since the testing facility may be covered as a provider, this release should be endorsed by employees **BEFORE** these examinations and testing occurs. This way, there will not be any "snags" when the employer wants to receive the results of the test. Too many times, testing facilities have refused to release the results of the tests to the employer since no Authorization and Disclosure Agreement exists. Again, even if the employer is not covered by HIPAA, the testing facility may be covered.

(Also, if the employer does use its insurance provider to pay for pre-employment medical examinations, "Fit-To-Return-To-Work" medical examinations, or substance abuse testing, then the employer is covered by HIPAA. The job applicant or employee should also be given a copy of the company's "Notice of Privacy Rights" and the "Notice of Confidentiality of Alcohol and Drug Abuse Testing Rights.")

These forms should therefore be loaded into your computer system and used when needed.

J. Confidentiality Agreement *(Used By Employers Covered By HIPAA And NOT Covered By HIPAA)*

Anyone who has access to Personal Health Information should endorse a Confidentiality Agreement. This document should then be filed in their personnel file.

It is also a good idea to have anyone who has access to medical or other types of confidential information to endorse a Confidentiality Agreement.

K. "Business Associate Agreements"

Human resources should also begin to identify all of the organization's "business associates" who receive protected health information ("PHI") from or on behalf of the plan. The organization's TPA, broker or an attorney could be business associates. Once these business associates are identified, the organization must have them execute a "business associate contract" before it discloses any PHI to them. Typically, these Business Associate Privacy Agreements should include many items, such as:

1. Identify the Business Associate and his/her role,

2. State his/her obligations under HIPAA regarding protected health information,

3. State that the Business Associate agrees to use appropriate safeguards to protect the PHI, and

4. Identify the proper uses of PHI by the Business Associates.

L. Privacy Policy

Covered organizations must draft and adopt a "Privacy Policy" and disseminate this information to anyone on whom it maintains PHI records. This Privacy Notice should at a minimum:

1. Identify the privacy safeguards that have been taken by the organization in order to put forth a "good faith effort" to ensure that the individual's protected health information will be secured,

2. Specify how an individual's protected health information will be stored, transmitted, and used or disclosed, which includes electronic, written and oral transmissions, and what safeguards have been adopted to ensure confidentiality,

3. Ensure that all "Business Associates" that receive this information will be subject to the same "Confidentiality and Privacy Requirements" as internal staff,

4. Ensure that all staff members that have access to this information will endorse a "Confidentiality Agreement,"

5. Ensure that PHI records will not be used in connection with any employment-related action or decisions, or in connection with any other benefit or benefits plan, except where allowed by law,

6. Ensure that any misuses of PHI records or any disclosures that are inconsistent with the purpose for which it was provided will be reported to the organization's Privacy Officer and/or the plan sponsor, which either is appropriate,

7. Review what rights individuals have under the HIPAA regulations,

8. Identify the penalties for violating the Privacy Policy,

9. Identify the organization's Privacy Officer and what role this person plays in ensuring maintaining the confidentiality of PHI records and HIPAA compliance,

10. The complaint procedure individuals should follow if they feel their rights have been violated and

11. Ensure that all employees will have access to their PHI records upon request and the procedure employees should follow in order to request such information.

The Privacy Policy statement should be signed by the organization's chief executive officer.

This Privacy Notice must then be communicated to anyone on whom the organization maintains PHI records. Employers should also obtain a written acknowledgment from its patients, consumers or employees that they have received a copy of its Privacy Notice.

Certain areas of compliance that should be included in the organization's Privacy Policy that deserves specific mention in more detail are as follows:

1. PHI Records Release

Disclosures of health information should be limited to the minimum amount necessary for specified purposes. Disclosures for public health or law enforcement purposes are permitted when required or permitted by law.

This rule requires that anyone maintaining PHI records must obtain special written authorization from patients before using any "protected health information" for anything besides treatment, payment or health care operations. It is important to note that healthcare providers, such as physicians and other medical providers generally must obtain an individual's written consent before making any uses or disclosures of the information.

Therefore, employers must have "Authorization to Release Medical/Mental Information" forms ready to send to health care providers in order to receive leave information regarding FMLA, ADA, pregnancy, etc. Otherwise, healthcare providers may not be able to provide the necessary information to the employer.

Patients, which may also be employees, must be given a clear written explanation of how their health information will be used or disclosed, with such use or disclosure generally occurring only upon the patients' written consent. Prior consents that provide equal or better protection may be relied upon.

It is also important to note that employers are not permitted to force employees to sign these releases. Forcing employees to release such information for such purposes is a violation of HIPAA.

2. Patients' Right Of Access

Patients must be given the right to have access to their own medical information and may request an amendment to records and restrictions in use. A complaint procedure must be provided to resolve privacy violations.

The HIPAA regulations therefore any removes any previous mandatory consent requirements that prevent the patient's access to their own health care records.

3. Complaint Procedure

HIPAA's "Privacy Standard" requires that covered organizations draft, implement and communicate a complaint procedure for responding to any complaints lodged by patients, consumers or employees regarding the safeguarding of their protected health information.

M. Corporate Privacy Officer

Any organization that has access to any protected health information ("PHI") must appoint a company "Privacy Officer." The duties of the Privacy Officer should be outlined in a job description, which includes such duties as:

1. Maintaining compliance with federal and state privacy laws,
2. Develops policies and procedures that provide safeguards for PHI,
3. Develops policies and procedures for reporting violations,
4. Establishes internal audit procedures to ensure compliance and
5. Trains employees who handle PHI regarding the proper procedures to follow in order to ensure its privacy.

N. Required Training

Training the organization's staff on its "Privacy Policy" and its procedures is a specific requirement of the Privacy Rule. Organizations are required to provide a detailed training session to all staff members who have access to protected health information addressing at least the following areas:

1. HIPAA's Privacy Rule,
2. HIPAA's penalties for non-compliance,
3. A review of the organization's privacy procedures,
4. The forms and disclosures used by the organization for compliance and
5. The system the organization has adopted for documenting compliance.

It is also important to document all of the training staff members receive regarding HIPAA by stating the topics covered and individuals who participated.

Employees who do not have access to PHI records should be trained regarding the organization's Privacy Policy and their rights under the law.

O. HIPAA's Electronic Data Interchange ("EDI") Rule

As of October 16, 2002, any organization transferring or storing PHI electronically were required to ensure that the proper firewalls were in place to protect this sensitive information.

P. HIPAA'S Security and Electronic Signatures Rule

Organizations are also required to:

1. Establish and maintain personnel security policies,
2. Establish and enforce physical security requirements, which may include access controls,
3. Audit controls and procedures,
4. Authorization controls and
5. Data and entity authentication controls.

Q. Checklist For Compliance

Covered organizations should examine the following checklist in order to begin complying with HIPAA:

1. Develop a Privacy Policy, along with the necessary procedures, including implementation deadlines.

2. Develop a budget for HIPAA compliance expenses, which would include attorney assistance, training, administrative assistance, copying, etc.

3. Review and revise group health plan documents in order to ensure that the necessary HIPAA privacy language is in place.

4. Appoint a HIPAA Privacy Officer.

5. Obtain "Business Associate" agreements wherever appropriate.

6. Train key managers regarding the organization's Privacy Policy, its procedures, the scope of HIPAA's rules and the consequences of noncompliance.

7. Conduct in-depth training for all staff members who will have access to PHI records, which at a minimum includes the organization's Privacy Policy, the organization's security procedures, its documentation procedures, the scope of the HIPAA rules and the consequences of noncompliance.

8. Train all employees regarding the organization's Privacy Policy and its procedures in accordance with HIPAA's regulations.

9. State in the employer's "Disciplinary Policy" clear sanctions for anyone who violates the organization's Privacy Policy or its procedures.

10. Ensure that appropriate security safeguards have been put into place, such as firewalls, access codes, Confidentiality Agreements endorsed, Business Associate Agreements endorsed, etc.

R. Penalties Under HIPAA

HIPAA prohibits retaliation against employees who refuse to sign authorizations that allow additional, specific uses of health information beyond treatment, payment and health care operations. Employers should remember that they are prohibited from using any protected health information in relation making personnel decisions.

Although the Privacy Rule includes no authority for private lawsuits, significant penalties may be imposed for violations, including criminal sanctions. HIPAA violators face penalties of $100.00 for each violation from the Health and Human Services Office of Civil Rights up to a maximum of $25,000.00.

The maximum criminal penalties under HIPAA are:

1. $50,000 and one year in prison for obtaining or disclosing protected health information.

2. $100,000 and five years for obtaining protected health information under "false pretenses."

3. $250,000 and 10 years for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

WHAT DOES THIS MEAN TO HUMAN RESOURCES?

Human Resources have the necessary forms needed to comply with HIPAA. Those forms are listed below.

The nice aspect of HIPAA is that it is “form driven.” Once an employer has these forms in place, compliance is relatively simple.

One way to avoid being covered by HIPAA is to outsource many of these various functions to an insurance broker. (i.e., Cafeteria Plan Claims, Insurance Renewals, etc.)

However, even if an employer is able to avoid HIPAA coverage, Human Resource professionals must still have the following forms in their arsenal:

1. **Confidentiality Agreement**

2. **Authorization and Disclosure**

Even if the employer is not covered by HIPAA, medical professionals are covered. Too many HR people these days are not getting their "Leave Certification Requests" completed by physicians since no proper release exists. The idea is to keep the system moving smoothly. HR people should put the Authorization and Disclosure Release Form with their "Medical Certification" forms under the ADA and FMLA.

Further, it is just a good idea to have all supervisors and managers sign "Confidentiality Agreements." Too many times, management inadvertently says something about a person's vasectomy, miscarriage, etc. This agreement helps to remind managers that such information is confidential.

REMEMBER: HIPAA is not the only privacy issue out there. ADA has privacy restrictions, as do most states under "common law privacy" rights.

DOCUMENTS EMPLOYERS WILL NEED TO COMPLY WITH HIPAA

(Used By Employers Covered By HIPAA And <u>NOT</u> Covered By HIPAA)

1. **Confidentiality Agreement**
2. **Authorization and Disclosure**

(Used By Employers Covered By HIPAA)

3. **Privacy Policy**
4. **Job Requirements for Privacy Officer and Employees**
5. **Business Associate Agreement**
6. **Notice of Privacy Rights**

Notice: Legal Advice Disclaimer

The purpose of these materials is not to act as legal advice but is intended to provide human resource professionals and their managers with a general overview of some of the more important employment and labor laws affecting their departments. The facts of each instance vary to the point that such a brief overview could not possibly be used in place of the advice of legal counsel.

Also, every situation tends to be factually different depending on the circumstances involved, which requires a specific application of the law.

Additionally, employment and labor laws are in a constant state of change by way of either court decisions or the legislature.

Therefore, whenever such issues arise, the advice of an attorney should be sought.

Scott Warrick, JD, MLHR, CEQC, SPHR

Scott Warrick's Consulting & Employment Law Services

(614) 367-0842 Office ♣ (614) 738-8317 Cell ♣ (614) 367-1044 FAX

www.scottwarrick.com

CEO Magazine's 2008 Human Resources "Superstar"

Nationally Certified Emotional Intelligence Counselor

2008, 2007, 2006 and 2003 SHRM National Diversity Conference Presenter

Scott Trains Managers and Employees ON-SITE in over 40 topics

Scott uses his unique background of **LAW** and **HUMAN RESOURCES** to help organizations avoid legal pitfalls while also helping them improve their employee relations and communication skills.

Scott travels the country presenting his revolutionary **"Emotional Intelligence, Tolerance & Diversity for White Guys … And Other Human Beings: FINALLY A Program For Everyone."** This one of a kind **SKILL-BASED** program creates an atmosphere of open communication so we are better able to resolve all kinds of conflicts in our organizations.

Scott's unique program is the ONLY Diversity/Tolerance Program in the country approved by HRCI-SHRM for STRATEGIC SPHR Credit because unlike most other EI/Diversity/Tolerance Programs, this program goes right to YOUR BOTTOM-LINE.

Scott's clients include the Adena Health Systems, St. Rita's Hospital, Ohio Department of Administrative Services, the Office of Housing and Urban Development, the Bayer Corporation, The Ohio State University, Area Agency on Aging, the Nebraska Army/National Guard, Heinz Frozen Foods, Boeing, EBMC, Honeywell, International Truck & Engine, MTD Products (Cub Cadet, Troy-Bilt & Bolens Lawn Products), etc.

Scott's academic background and awards include:

- Capital University College of Law (Class Valedictorian (1st out of 233))
- Master of Labor and Human Resources and B.A. in Organizational Communication: The Ohio State University
- The Human Resource Association of Central Ohio's Linda Kerns Award for Outstanding Creativity in the Field of Human Resource Management and the Ohio State Human Resource Council's David Prize for Creativity in Human Resource Management

Solving Employee Problems BEFORE They Happen!