WIMBERLY LAWSON
SEALE WRIGHT & DAVES, PLLC
ATTORNEYS & COUNSELORS AT LAW

THE EAGLE'S VIEW

April 2004 Volume 4, Issue 4

A LAYMAN'S GUIDE TO BEGINNING HIPAA COMPLIANCE

BACKGROUND

Final regulations were published by the Department of Health and Human Services on December 28, 2000 to implement the health information privacy mandates of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Small health plans with not more than $5 million in annual receipts have until April 14, 2004 to come into compliance with the Privacy Rules of HIPAA. The basic principle of the Rules is that a covered entity may use or disclose "protected health information" only if the individual who is the subject of the information consents or authorizes the use in writing, or as the Privacy Rules permit or require. The Rules require covered entities to adopt comprehensive policies and procedures to safeguard "protected health information" (PHI) and to inform, and preserve the rights of, the individuals who are the subjects of this information.

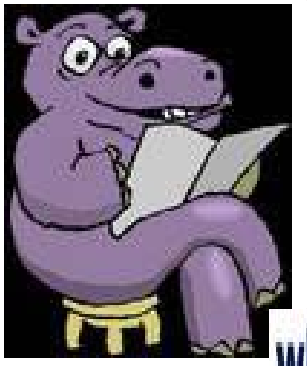
The Privacy Rules are applicable to covered entities, which are defined as health plans, health care clearing houses and most health care providers who conduct certain financial and administrative transactions electronically. Employers or plan sponsors who provide self-funded health plans are not considered to be covered entities, but the group health plans they establish for their employees are covered entities. ERISA plans are also considered to be health plans as defined by HIPAA. In addition to the covered entity status as health plans, employers who offer certain health care services may also qualify as covered entities. The Privacy Rules specify that the following are not covered health plans: insurers of "excepted benefits" - disability income, workers compensation, automobile medical payment, general and automobile liability, credit-only, life and similar coverage where any medical benefits are "secondary or incidental to other insurance benefits."

PHI includes all individually identifiable health information that is maintained or communicated in any form by a covered entity. However, PHI does not include employment records held in an employer capacity, as opposed to health plan capacity.

If the employer group health plan is fully insured, and the plan has elected to receive only summary health information and de-identified PHI, it will likely fall under the insurer's HIPAA privacy umbrella, meaning that the responsibility to comply with HIPAA will fall on the insurer. However, if fully-insured groups elect not to receive PHI, they should formally document this decision and modify any of their existing practices that currently involve the use of PHI.

Fully-insured groups that have access to PHI (other than enrollment/disenrollment and eligibility data and summary health information) must fully comply with the provisions of the privacy regulations. Similarly, self-insured groups must fully comply with all provisions of the privacy regulations.

Although self-insured groups must comply with all provisions of the privacy regulations, they may be able to reduce the actual amount of administrative work they must do by limiting the amount of PHI that their employees use or disclose. For example, most self-insured groups hire a third party administrator (TPA) to administer their health plans and the group elects to receive only enrollment and eligibility data and summary health information. Because the administrative responsibilities for a plan required by HIPAA can normally be included in a business associate contract between the group health plan and the TPA, the administrative burden for such a group to comply with the regulations



About our Firm

Wimberly Lawson Seale Wright & Daves, PLLC is a full service labor, employment and immigration law firm representing management exclusively. The firm has offices in Knoxville, Morristown, Cookeville and Nashville, Tennessee and maintains its affiliation with the firms of Wimberly, Lawson, Steckel, Nelson & Schneider, P.C., Atlanta, Georgia; and Wimberly Lawson Daniels & Brandon, Greenville, South Carolina.

Locations

Knoxville Office
Bank of America Building, Suite 900
550 Main Avenue
P. O. Box 2231
Knoxville, Tennessee 37901-2231
Phone: 865-546-1000/Fax: 865-546-1001

Morristown Office
929 West First North Street
P.O. Box 1066
Morristown, Tennessee 37816-1066
Phone: 423-587-6870/Fax: 423-587-1479

Cookeville Office
1420 Neal Street - Suite 201
P.O. Box 655
Cookeville, Tennessee 38503-0655
Phone: 931-372-9123/Fax: 931-372-9181

Nashville Office
200 Fourth Avenue South
Suite 900
Nashville, Tennessee 37219
Phone: 615-727-1000/Fax: 615-727-1001

Website: www.wlswd.com

Affiliated Offices
Wimberly, Lawson, Steckel, Nelson & Schneider, PC
Atlanta, Georgia

Wimberly Lawson Daniels & Brandon
Greenville, South Carolina

Wimberly, Lawson, Suarez & Russell, LLC
Tampa, Florida

Inside.....

is much less than if the group plan receives PHI on individual members and the treatment they receive.

The privacy regulation has a significant impact on the information that can be made available to the employer, who is usually the plan sponsor. Group health plans may not disclose their enrollees' PHI to the employer or the plan sponsor, although the employer/plan sponsor may receive summary health information from the group health plan or insurer for the limited purpose of obtaining bids on the plan's health insurance coverage or for the limited purpose of modifying, amending or terminating the health plan. There is an exception to the prohibition of making PHI available to the plan sponsor (i.e., the employer), when the employer/plan sponsor performs "plan administrative functions" for the health plan (such as case management, utilization review, overpayment recovery, reimbursement, benefits administration, etc). However, even if the group health plan or insurer discloses PHI to the employer for such plan administrative purposes, it may only be done if the plan documents are amended to include certain required provisions, including a description of the employees or workforce members that the plan sponsor has given access to member PHI, and the PHI must be safeguarded per the requirements of the privacy regulations.

Regardless of whether the employer/plan sponsor has an insured or self-insured plan, a great deal of coordination is necessary with the TPA to comply with HIPAA. A practical problem is that the TPA does not want to be in a position of providing legal advice to the employer. However, TPAs are often able to provide sample plan documents and compliance checklists. TPAs will not, however, review or monitor the employer/plan sponsor's obligations, and there is no formal certification process for the employer to insure that its health plans are in compliance. The main concept for the employer is to take reasonable actions to meet the intent of the regulations, and to have proper rules and procedures in effect, all in writing.

SMOKY MOUNTAIN AND MUSIC CITY FALL CONFERENCES

October 28 and 29, 2004
Knoxville, TN

November 18 and 19, 2004
Nashville, TN

So you won't miss these informative seminars, be sure to mark your calendars now. Details will be available soon.

KNOW YOUR ATTORNEY

JEFFREY C. TAYLOR

Jeff is a regional managing member of the firm and has been with the firm since 1990. He received his Bachelor of Science degree in Business Administration from East Tennessee State University in 1985 and his law degree from University of Memphis, Cecil C. Humphreys School of Law in 1988. Jeff is headquartered out of the Morristown office. His experience and practice areas include employment law, wage and hour, wrongful discharge, ADA, workers' compensation, FMLA litigation and compliance counseling, union avoidance, and business law.

Jeff is a member of the Hamblen County, Tennessee and American Bar Associations. After private practice in 1988, he served as Assistant Public Defender, 4th Judicial District of Tennessee, from 1989 until 1990. Fraternities: Phi Alpha Delta (Justice 1987-1988). Community Activities: 1998, 2002 Legal Advisor to Morristown Chamber of Commerce; 2003 Vice President of Leadership Division, 2003-2004 Board of Directors Morristown Area Chamber of Commerce; Kiwanis Club of Morristown; 2003-2004 Board of Directors Kingswood School, Inc.; 2003-2004 Board of Directors Healthstar Foundation; 2003 Professional Division Chair - Hamblen County United Way; Advisor Boy Scouts of America-Explorer Division (1992-1997). 1992-1997 Board of Directors Rose Center; Council for the Arts, 1997 Chairman. (Morristown, Tennessee).

Jeff and his wife, Ashley, live in Morristown, enjoy playing tennis and golf, and are the proud owners of two dogs, Louie and Sissy.

HIPAA - COMPLIANCE CHECKLIST

- ✔ Adopt written privacy policies and procedures that define access to PHI, the use of PHI by the covered entity, and the process for disclosure of PHI.
- ✔ Take steps to insure that business associates, such as the TPA, adequately provide for the confidentiality and privacy of PHI, and enter into a Business Associate Agreement specifying the details of the relationship regarding the use and/or disclosure of PHI.
- ✔ Establish procedures that provide a means for enrollees to make inquiries or register complaints regarding the privacy of the records.
- ✔ Establish procedures that provide a means for enrollees to access, make copies of and request amendments to their records.
- ✔ Designate a privacy official to be responsible for insuring the organization's privacy procedures are followed.
- ✔ Provide a notice of privacy practices to enrollees.
- ✔ Train employees on the basic provisions of the privacy regulation and the organization's privacy policies and procedures.
- ✔ Establish sanctions for employees who violate privacy policies and procedures.

HIPAA - PRACTICAL ADVICE

The simplest way to come into compliance is to purchase a set of forms and then adapt the forms to the employers' individual situation and their relationship with their Business Associates, such as their TPA. A great deal of individual adaptation is necessary. The plan needs to decide how much it wants to be involved in plan administration. For example, an employee may want certain PHI related information from the plan and the plan needs to decide whether to receive the information from the employee, call the TPA, get the information from the TPA, provide it to the employee, or alternatively tell the employee to contact the TPA for the information. Similar issues will arise when an employee requests access to PHI or an amendment to PHI. State law may also need to be considered since many states have laws dealing with access to PHI. It is obviously easier for the plan to simply refer the employee to the TPA, or forward the request to the TPA, rather than to get involved. On the other hand, some plans like to assist employees in claims processing. A compromise procedure might be to adopt HIPAA policies that if the TPA cannot resolve the matter in 30 days the employee should contact the privacy officer, who will contact the TPA for assistance. The HIPAA policies must address the procedures as to how these matters will actually work.

Similarly, the HIPAA plans and procedures must designate a privacy officer or office, a person or office to whom complaints may be made about PHI matters. Many plans will choose to have the same individual or office hold both positions. It is usually easier to designate an office or officer in the plan documents, as opposed to an individual, in case the individual is no longer employed by the employer or is unavailable.

The privacy officer could be a part of HR, and the employer could have the same person wearing two hats - an HR hat and a privacy officer hat, or use two different people or positions. The employer's normal way of doing things should be considered in making these decisions, as perhaps the person who receives complaints about benefits claims issues or who solicits bids for insurance should be the privacy officer. It is desirable that this benefits handler have a "fire wall" created to keep the PHI information separate from those people who make HR decisions. In order to draft the various plans, employers need to map out the flow of PHI information in their particular companies, who sees or handles it, who has access to it, so that the various privacy policies can be drafted and implemented. One way to look upon the issues is to consider PHI as a trade secret and to look at the company's policies and procedures on trade secrets and apply some of those standards to PHI. In April 2005, a separate set of policies and procedures will be necessary due to the security rules that will go into effect then, that are similar to the privacy rules that are already in effect.

Much of the information exchanged between the plan and the TPA will be information related to the treatment of that individual, or payment for the treatment, and the plan needs to cover its role in treatment, administrative claims and payments. This is basically an access issue as to who can have access to this type of information. The totality of this type information is probably not PHI, but if details have been provided such as the names of individuals or a way in which the individuals can be identified, the information will be subject to the privacy rules. For example, if accounting needs to have the names, diagnoses, and the like, possibly for purposes of double-checking the payments, that person in accounting may need to be added to the plan and provided a job description and training concerning PHI. PHI can only be shared with a person that is part of plan administration, or otherwise there must be authorization from the employee or person receiving the treatment. If there is an unauthorized disclosure, it must be investigated, mitigated and discipline needs to be considered as to the person committing the violation. All of these things need to be a part of the plan's written policies and procedures. The various policies and procedures to comply with HIPAA can either be in one document, or in a series of documents.

The simplest way to come into compliance is to purchase a set of forms and then adapt the forms to the employers' individual situation and their relationship with their Business Associates, such as their TPA.

The TPA will only talk to the people at the plan who are designated or who have positions so designated to receive information from the TPA. For example, if the person paying the bills needs reports from the TPA, that person needs to be identified to the TPA. If the information provided goes beyond normal claims processing information, it would require special written authorization to release the information from the enrollee.

Health plans must distribute their privacy notice to each of their enrollees by the compliance date, which for plans of less than $5 million in revenue is April 14, 2004. The Notice of Privacy Practices is important, not only because it is legally required, but also because the plan must always comply with the content of its Notice (much like a contract). Thereafter, health plans must distribute their privacy notice to each new enrollee. The health plan must distribute a revised notice to each of its enrollees within 60 days after a material change in its privacy practices. The health plan satisfies its distribution obligations by giving its notice and its periodic reminder to the enrollee, even though its coverage may also apply to a spouse and one or more dependents.

A covered entity must train all workforce members receiving PHI on its privacy policies and procedures. Initial privacy training must be completed by the Privacy Rules compliance date. Thereafter, each new workforce member must receive privacy training appropriate to the position within a reasonable time after employment starts.

Wimberly Lawson
Seale Wright & Daves, PLLC
Attorneys & Counselors at Law
P.O. Box 2231
Knoxville, Tennessee 37901-2231
Visit our Website at http://www.wlswd.com

RETURN SERVICE REQUESTED

PRSRT STD
US Postage
PAID
Permit 582
Knoxville, TN
37950

****

CHANGES TO SUBSCRIPTION
If you would like to change your address or unsubscribe to this publication, please visit the newsletter portion of our website (wlswd.com). A special link has been provided. OR, you may call Brenda Hopper at 865-546-1000.

****

HIPAA - SPECIAL ISSUES

A health care provider, such as a plant nurse, who is a member of an employer's workforce, or who provides health care to individuals at an employer's request, is permitted to disclose PHI to the employer without the individual's authorization. Disclosure is limited to situations involving medical surveillance of the workplace or evaluation of an individual for work-related illness or injury and to the PHI derived from these situations. A health care provider is required to give the individual written notice of protected health information to be disclosed to the employer. This notice must be given at the time health care is provided, or if care is provided at the employer's work site, by posting a notice at a prominent place at the site. These same concepts may apply to any other employer-provided medical and health services, such as on-site health clinics, wellness programs, disease management programs, employee assistance programs, and occupational health and medicine services, but careful review to determine compliance with HIPAA and state law is necessary.

Information received by the employer as an employer is not covered by HIPAA. However, some employers are electing, although are not required to treat health-related workers compensation and employment information (i.e. requests for medical leave, etc), like PHI information, and cover it under HIPAA for convenience. Even if such employment-gained information is not covered under HIPAA, there are related privacy rules under the Americans With Disabilities Act, that must be met.

Special issues deal with electronic PHI on the server, as IT persons can get access to this information. The employer will have to use a limited access file or put the responsibility in the job description of all IT persons with such access and provide them with training and non-disclosure statements for them to review and certify as having received the policies, procedures, and training.

E-mails also present special issues. E-mails are not secure, and therefore one possible policy is not to communicate PHI information over E-mails. The alternative is to communicate PHI information under special attachments that are password-protected. One of these approaches has to be covered in the written HIPAA policies and procedures. Fax machines are another special problem. While they may be used, there must be written policies on such use of communicating PHI information. For example, the policies must cover how long such information will be left on the fax machine, the cleaning off of desks in the evening, putting the pertinent fax machine in a limited access area with a locked door, and all of the policies and procedures must be in writing.