CROSS, GUNTER, WITHERSPOON & GALCHUS, P.C.

ATTORNEYS AT LAW
LITTLE ROCK/FORT SMITH/FAYETTEVILLE

www.cgwg.com

Scotty Shively
sshively@cgwg.com

500 President Clinton Avenue, Suite 200
Little Rock, AR 72201
Telephone (501) 371-9999
Fax (501) 371-0035

Mailing Address
P.O. Box 3178
Little Rock, AR 72203

AMERICAN BAR ASSOCIATION 2004 ANNUAL MEETING
ATLANTA, TUESDAY, AUGUST 10, 2004

SECTION OF EMPLOYMENT AND LABOR LAW

DO YOU WANT TO KNOW A SECRET:
HIPAA AND THE NEW MEDICAL INFORMATION PRIVACY REGULATIONS

HIPAA FOR EMPLOYERS

Presentation by Scotty Shively

HIPAA Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) amended five federal statutes. It provided for portability of health coverage, added an arsenal of laws to the government for fighting fraud and abuse in public health plans, and provided for administrative simplification in processing of health care claims. HIPAA's administrative simplification provisions were designed to improve the efficiency and effectiveness of the health care system by facilitating the electronic exchange of information with respect to financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with these transactions.

The Administrative Simplification provision raised a concern about the privacy of an individual's health information. The Act promulgated standards and empowered the Department of Health and Human Services (DHHS) to issue regulations if Congress had not enacted privacy legislation by August 21, 1999. Congress failed to act by the deadline and the DHHS issued proposed regulations on November 3, 1999. The final regulations for the standards for privacy of individual identifiable health information were issued on December 28, 2000, in the last days of the Clinton administration. This final rule was the subject of much debate among members of the health care community and advocates of privacy rights. DHHS published a modified Final Rule on August 14, 2002. This Privacy Rule deals only with a very narrow provision in the Administrative Simplification title – Title II – and is only one of

five standards which addresses Administrative Simplification. However, the Privacy Rule is the tail that wags the HIPAA.

The Administration Simplification provisions of HIPAA (Title II) include HIPAA Privacy Rule, HIPAA Security Rule, and the Transactions and Code Set Standards.

The Privacy Rule requires the adoption of comprehensive privacy policies and procedures to safeguard protected health information ("PHI"). The Privacy Rule allows use or disclosure of PHI in the following situations:

- to the person who is the subject of the PHI (45 C.F.R. §164.502(a)(1)(i));
- to carry out treatment, payment or health care operations ("TPO") (45 C.F.R. §164.502(a)(1)(ii));
- pursuant to an allowed exception (45 C.F.R. §164.502(a)(1)(iii));
- pursuant to a valid authorization (45 C.F.R. §164.502(a)(1)(iv));
- where the PHI has been de-identified (45 C.F.R. §164.502(a)(2)).

The Privacy Rule became effective on April 14, 2003 for providers, clearing houses, and health plans of over $5 Million; it became effective for health plans of $5 Million and under on April 14, 2004.

The Security Rule protects electronic information or information transmitted electronically. The Security Rule requires Covered Entities to promulgate a risk management program to evaluate the value of the assets, the potential for a loss or disclosure, and the cost of additional countermeasures. The Security Rule becomes effective on April 20, 2005, except for small health plans which have until April 21, 2006.

HIPAA Privacy Rules and Security Rules are not identical so using the same policies and procedures for both will not work. The Privacy Rules are concerned with "what and why" all health information, electronic and non-electronic, is protected; the Security Rules deal with "how" election information is protected.

The Transactions and Code Set Standards established standardized computer formats and medical codes for specified billing and claims administration transactions. This phase applies to Covered Entities with an effective date of October 16, 2002 (October 16, 2003 for small health plans).

Purpose of HIPAA Privacy

Prior to passage of HIPAA, there was no comprehensive federal law that addressed the use and disclosure of patient health care and payment information. State laws were inconsistent and contradictory, only covered specific types of records (e.g., HIV/AIDS), or did not exist at all. Many state laws fail to provide such

basic protection as ensuring a patient's legal right to see a copy of his or her own medical records. (65 F.R. 82463-464). Factors adding to the concern over confidentiality of medical information were the growth in the number of companies providing care and processing claims, growth in use of electronic information technology (electronic claims processing and access to the internet), and increasing ability to collect highly sensitive information as a result of advances in scientific research. (65 F.R. 82463).

Important Dates and Deadlines for Administrative Simplification Provisions

August 21, 1996	HIPAA enacted; contains "Administrative Simplification" provisions	42 U.S.C. §§1320d-2 et seq.
Dec. 28, 2000	Final Privacy Rule published by Clinton Administration	65 F.R. 82462
August 14, 2002	Final Privacy Rule (as modified)	67 F.R. 53182, 45 C.F.R. § 160, 164
October 16, 2002	Compliance deadline for electronic transactions (unless extended)	
Feb. 20, 2003	Final Security Rule published	45 C.F.R. §§160.103, 162.103
April 14, 2003	Final compliance with Privacy Rule for all covered entities except "small health plans"	45 C.F.R. § 164.534
April 14, 2004	Final compliance with Privacy Rule for "small health plans" ($5 Million or less) effective date	45 C.F.R. § 164.534(b)(2)
July 30, 2004	Employer Identifier Standard – all covered entitles except small health plans - effective date	67 F.R. 38009
April 20, 2005	Final compliance with Security Rules (except for small health plans)	45 CFR §164.318
August 1, 2005	Employer Identifier Standard for small health plans	
April 21, 2006	Final compliance with Security Rule for small health plans	
May 23, 2007	Final compliance re: National Provider Identifier for all but small health plans	69 F.R. 3434
May 23, 2008	Final compliance re: National Provider Identifier for small health plans	

Who is covered by the Administrative Simplification Standards of HIPAA?

In 45 C.F.R. §160.103, "Covered Entities" are defined as:

- Group health plans
- Health care clearinghouses
- Health care providers that transmit information in electronic form
- Employers, in their role as employers, are not one of the defined "covered entities."

Employers are indirectly regulated by HIPAA if they are a plan sponsor of ERISA health plans.

HIPAA'S Application To Employers

Employers were one of the first groups to gain awareness of the HIPAA Act because the Title I portability provisions became effective in 1998. Employers who offered health insurance to employees concentrated on the provisions relating to special enrollment periods, certificates of creditable coverage, and other provisions related to the portability of coverage.

Employers may be directly covered as a provider entity if they have an on-site health clinic or provide on-site healthcare services for which they bill electronically. However, most employers are indirectly covered because they sponsor employee health plans that are covered entities. The extent to which employers are impacted depends upon whether the group health plan is fully-insured or self-insured.

Employers are impacted by HIPAA because they often need protected health information (PHI) about an employee which is maintained by a covered entity. Finally, employers are impacted because HIPAA has created a heightened sense of privacy not only for medical records, but for other information pertaining to employees and other individuals.

HIPAA Basics for Privacy Rule

Covered Entities (defined at 45 C.F.R. §160.103)

The first step in HIPAA analysis is determining whether an employer is a covered entity. A covered entity includes health plans, health care clearing houses, and health care providers who transmit any health information in electronic form. It is important to note that this electronic transmission condition applies only to health care providers. Health plans and health care clearing houses are covered regardless of whether they transmit in electronic form.

A health care provider is defined as a provider of medical or services described under Medicare Part A or Part B (which encompasses most typical health care services) or any other person or organization that furnishes, bills, or is paid for health care in the normal course of business.

A health care clearinghouse is an entity, such as a billing service, repricing company, or value-added network that either processes the health information received from another entity into a standard transaction or receives a standard transaction and processes it into nonstandard data content.

A health care plan is defined as any individual or group that provides or pays for the cost of medical care. This includes HMOs, Medicare and Medicaid plans, issuers of health insurance, Medicare supplemental-care policies and long-term care policies, ERISA employee welfare benefit plans, active military personnel health care programs, veterans' health care programs, and others. Specifically excluded from the definition of health plan, even though they may provide for the payment of medical care, are Workers' Compensation plans, casualty and property insurance plans, and disability insurance programs. An employer health plan with fewer than 50 participants and which is self-administered by the employer is also excluded from the definition of health plan.

Protected Health Information (PHI) (defined at 45 C.F.R. § 160.103)

Protected health information (PHI) is individually identifiable information, including demographic information, related to the past, present, or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for such health care, that is created or received by a covered entity. Individually identifiable information (45 C.F.R. § 164.514(b)(2) covers a broad range of identifiers of the individual, his relatives, employer or household members, including:

- name, address, telephone numbers, and email addresses
- social security number
- account numbers used to identify the patient in medical records, health plans
- certificate/license numbers, vehicle and device identifiers, serial numbers
- biometric identifiers (finger/voice prints), photographic images
- all elements of dates (except year) including birth date, admission date, discharge date, date of death, and all ages over 89

Medical information found in employee records is not PHI. There is also an exception for medical information created pursuant to work place surveillance obligations which is discussed in more detail later in this presentation.

Employer-Sponsored Health Plan

Although most employers are not covered in their role as an employer, they may sponsor employee health plans which are covered entities. In addition to sponsoring a plan, the employer may also be a plan administrator and plan fiduciary

under ERISA. HIPAA recognizes that, under ERISA, a plan and its plan sponsor are separate legal entities. However, in practical terms it is the plan sponsor, *i.e*., the employer, that typically acts on behalf of the plan because the plan has no employees. Therefore, it will be the employer's responsibility as the plan sponsor and fiduciary to ensure the plan's compliance with the HIPAA regulations. An employer must examine each benefit it offers (i.e., major medical, dental, optical, EAP, health reimbursement account, flexible spending account, and specialty medical policy such as cancer policy) to determine if it meets the HIPAA definition of a health plan and, if so, examine the employer's responsibilities under HIPAA. These responsibilities can vary from plan to plan.

Employers offering self-insured health plans will be the most directly affected. They will be responsible for the plan's full compliance with HIPAA regulations, even if they use a TPA for plan administration. Employers offering fully insured plans will be able to delegate many compliance functions to the insurer but the employer's group health plan will retain some responsibilities.

1. Self-Insured Health Plans

In general, a self-insured or self-funded group health plan sponsored by an employer must comply with all health plan requirements under the Privacy Regulations. There is an exception for self-insured, self-administered plans with under fifty participants. The following are key provisions which apply to all health plans, but raise special issues in the context of an employer-sponsored health plan:

a. Notice of Privacy Practices (NPP). The group health plan must have a notice of privacy practices available for any enrolled participants. The notice be distributed only to named insured, i.e. employees, but not to dependents. The notice must state that the health plan, or the health plan's insurer or HMO may disclose PHI to the employer, as plan sponsor, for plan administration functions. *See* generally, 45 C.F.R. § 164.520.

NPP must be provided no later than the compliance date for the health plan (generally April 14, 2004), to new employees at the time of enrollment, and within 60 days of a material revision of the notice to individuals then covered by the plan. At least every three years the plan must notify covered individuals of the availability of the NPP and how to obtain the notice. 45 C.F.R. § 164.520(c)(1).

b. Authorizations. A health plan does not need an individual's consent or acknowledgment of its notice of privacy practices to use or disclose PHI for treatment, payment, or health care operations. (45 C.F.R. § 164.506.) These activities include claim payment, stop-loss claims, subrogation, evaluating plan performance, underwriting, auditing, and medical reviews. A number of other disclosures do not require consent or authorization, including disclosures to comply with Workers' Compensation laws. 45 C.F.R. § 164.510 and .512.

Other uses and disclosures of information by the health plan require a written authorization from the individual. *See* 45 C.F.R. § 164.508. Examples of uses/disclosures that would require such authorization include any disclosures by the health plan to the plan sponsor for non-plan purposes or providing names of individuals covered by the medical plan to a long-term care insurer for marketing purposes. Employers should conduct an inventory of the plan's PHI uses and disclosures to determine which, if any, require such authorization.

c. Request for Access and Amendments; Accounting for Disclosures. (45 C.F.R. §§ 164.524; 526; and 528.) The health plan must establish a procedure for handling these requests. If most of the health plan PHI is held by a TPA, the TPA may perform these functions on behalf of the health plan. If so, these services should be made an obligation of the TPA under the administrative services contract, and appropriate policies and procedures should be developed. The ultimate responsibility for these functions remains with the health plan, however. The notice of privacy practices should explain whether individuals should contact the TPA or the employer with these requests.

d. Complaints. (45 C.F.R. § 164.530(d)) The health plan must establish a procedure to handle privacy complaints from individuals. The notice of privacy practices should explain whether individuals should contact the TPA or the employer with complaints.

e. Business Associate Agreements. (45 C.F.R. § 504(e)) A health plan will typically outsource some plan administration activities. Any outside entity that receives PHI from the plan in order to perform functions on behalf of the plan is a business associate of the health plan. Business associates may include, for example, TPAs, preferred provider organizations, utilization review companies, subrogation recovery firms, accounting firms, insurance brokers, consultants, and outside legal counsel. The plan must have the required business associate agreements in place with each such business associate. The business associate agreement provisions may be incorporated in another contract, such as an administrative services agreement with a TPA.

f. Administrative Requirements. The employer-sponsored health plan is also subject to the Privacy Regulations' administrative requirements. *See* 45 C.F.R. § 164.530. The plan must:

- Designate a privacy official;
- Document the plan's privacy policies and procedures;
- Conduct privacy training;
- Establish information security measures;
- Establish a system for reporting noncompliance; and
- Establish and enforce sanctions for policy violations.

In addition, to the requirements applicable to all health plans, the following are some special provisions that apply only to employer-sponsored health plans:

g. Limited Employer Access to PHI. (45 C.F.R. § 164.504(f).) Employers may not access any health plan PHI for non-plan purposes, and especially not for employment-related purposes. For example, an employer may not reassign an employee to another job based on information from the health plan that the employee is being treated for alcoholism. An employer receives personal information about the employees from a variety of sources, including directly from the employee. The concern of the Privacy Regulations, however, is information received from or through the employer's health plan.

h. Firewalls. Employers must establish a "firewall" between plan-related uses of PHI and general corporate or employment-related uses of PHI. 45 C.F.R. § 164.504(f)(2)(iii). Employers who currently have the same individual or group of individuals handling all benefit plans plus human resource matters should consider separating these functions. In small organizations where having different staff members for these functions is not feasible, the employer should, at a minimum, establish policies and conduct training regarding the confidentiality of PHI and the need to restrict uses as well as disclosures.

TPAs contacting an employer will need to be careful about the staff members at the employer's offices with whom they communicate, so that PHI is communicated only to authorized personnel. Covered entitles and business associates will need to carefully consider the appropriate avenues of communication.

Employment records are not PHI, even if they contain health information about an employee. Employment records are not subject to this HIPAA "firewall" requirement. Employment records may include medical information needed for an employer to carry out its obligations under the Family and Medical Leave Act, Americans with Disabilities Act, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees. Although not subject to the HIPAA "firewall," these type records have always been subject to "firewall" treatment under the Americans with Disabilities Act and must be kept separate from other personnel records.

i. Plan Document. The health plan's plan document must be amended to include a number of specific provisions relating to privacy. *See* 45 C.F.R. § 164.504(f). No disclosures from the health plan to the employer are permitted until the plan document is amended. The plan document must identify all permitted and required uses and disclosures of PHI by the employer for plan administration purposes. The plan document must state that the employer will not use PHI

received from the plan for employment-related actions or decisions, or in connection with any of the employer's other health plans. The plan document must identify which employees or classes of employees of the plan sponsor, or other persons under control of the plan sponsor, are to be given access to PHI (*e.g.*, a benefits clerk, a benefits committee, or claims appeal committee). In addition, the employer must ensure that there is adequate separation between the employer and the plan to protect the privacy of plan-held information.

2. Insured Health Plans

Employer-sponsored health plans that offer benefits through an insurance contract with a health insurance company or HMO (Insured Plans) are also covered entities under HIPAA. For Insured Plans, however, most of the compliance responsibilities discussed above will fall on the insurer or HMO, since they are already covered entities under HIPAA. For example, the insurer or HMO will typically provide the Notice of Privacy Practices and handle compliance with regard to the individual's right to access and amend their records, and to obtain an accounting of disclosures. The policy behind this limited-compliance approach for the Insured Plan is that the insurance company or HMO will be providing these individual rights and privacy protections in its own role as a covered entity, and the incremental value of having the employer's Insured Plan duplicate these activities would not justify the additional burdens on the plan sponsor. The obligations of an employer that sponsors an Insured Plan with regard to HIPAA compliance are determined by the approach the plan takes to PHI.

a. The Hands-Off Approach. Insured Plans can reduce their privacy obligations if they take a "hands-off" approach to PHI. An employer-sponsored health plan is not subject to most Privacy Regulations requirements if it provides benefits solely through an insurance contract with an insurer or HMO. To qualify under this "hands-off" approach, the Insured Plan may not create or receive any PHI, except in two limited situations. It may receive and use enrollment and disenrollment information and it may receive and use summary health information for the purpose of obtaining premium bids or modifying, amending, or terminating the plan. 45 C.F.R. § 164.504(f)(l)(ii). Even under this "hands-off" approach, there are two obligations on the Plan sponsor. It cannot retaliate against or intimidate an employee exercising his or her rights under the Privacy Regulations or require that an employee waive his or her right to file a complaint with DHHS as a condition for eligibility or participation in the plan. 45 C.F.R. § 164.530 (g), (b), (j), and (k). If the Insured Plan shares any PHI with the plan sponsor (employer) other than enrollment/disenrollment information and summary health information, the plan document must be amended as described above.

Most employers, as plan sponsors, have been more "hands on" in the past in helping employees with billing or coverage problems with either the insurance

company or the provider. A "hands off" employer must discontinue this practice unless it obtains a signed authorization from the employee.

b. The Hands-On Approach. If the Insured Plan does create or receive PHI in addition to enrollment/disenrollment and summary health information, *i.e.*, it takes a "hands-on" approach, it is generally subject to all of the Privacy Regulations requirements, including all of the administrative requirements discussed above, such as appointing a privacy official, documenting its policies and procedures, and providing training for its workforce. The responsibilities with regard to the notice of privacy practices are reduced, however. The Insured Plan must prepare and maintain a notice of privacy practices and provide that notice upon request (to anyone), but is not required to distribute the notice to all plan participants.

All health plans, including all Insured Plans, must limit employer access to PHI as described above and may not use health plan PHI for employment purposes.

Employer's Receipt and Use of Employees' Medical Information

HIPAA provides exceptions from the definition of PHI for medical information found in employee records (45 C.F.R. § 164.501) and for medical information created pursuant to OSHA medical surveillance obligations. (45 C.F.R. § 164.512(b)(1)(v))

Employers may have an obligation under OSHA or state laws to conduct medical surveillance on its employees. OSHA is authorized to adopt standards requiring medical screening and surveillance in certain industries. Medical screening is a method for detecting disease or bodily dysfunction in an individual without current symptoms, but who may be at high risk for certain adverse health outcomes. Medical surveillance, on the other hand, involves the analysis of health information to look for problems that may be occurring in the work place that require targeted prevention, and thus serves as a feedback loop to the employer. Thus, OSHA can require medical surveillance to determine whether a given occupation presents increased risks to employees, and, if it does, OSHA can then require medical screening of employees in that occupation to monitor their exposure to the increased hazards. Because an employer receives these medical records in its role as an "employer," it has no HIPAA responsibilities with respect to them. A provider, however, does have HIPAA responsibilities before it may release these medical records to an employer.

In order for a covered entity to disclose such information to the employer, several requirements must be satisfied. First, the covered entity must either be an on-site clinic or a clinic providing health care to an individual at the employer's request. The employer's request must be in relation to "medical surveillance of the workplace" or to evaluate whether the individual has a work-related illness or injury.

Second, the protected health information disclosed must consist of findings concerning work-related illness or injury or a workplace related medical surveillance.

Third, the employer must need such findings in order to comply with its OSHA or MSHA obligations, or similar state laws.

Finally, the covered entity must provide written notice to the individual that the PHI will be disclosed to the employer. This notice must be provided by the covered entity at the time of the treatment, or, if the covered entity is an on-site clinic, by posting the notice in a prominent place at the site.

Even though employers are not covered entities and information received in their employer role is not PHI, employers will still need a signed authorization to obtain PHI from a provider or group health plan since these are covered entities. This would include information from a provider such as fitness for duty, to make decisions about the employer's ADA accommodation responsibilities and results of drug screening. Any medical information provided directly by the employee such as off-work excuses, return to work slips, and FMLA certifications will not need an authorization.

Once a covered entity discloses PHI to another individual, such as the employer, the PHI loses its protection under HIPAA. However, the employer still has obligations under ADA and common law. An employer should not lose sight of the fact that even though HIPAA may not apply, HIPAA has raised the bar on employees' expectations of privacy with respect to their health information.

The HIPAA regulations have changed the way subpoenas for medical information are handled. If an employer receives a subpoena for production of an employee's health information, HIPAA does not apply unless the employer is self-insured and the subpoena requests health plan documents.

Workers' Compensation Issues

Even though a Workers' Compensation plan pays for medical care, it is not a covered entity. It is specifically exempted from the definition of group health plan. 45 C.F.R. § 160.102.

A Workers' Compensation carrier, third-party administrator, or self-insured employer can obtain medical records on a Workers' Comp claimant without obtaining an authorization. 45 C.F.R. § 512(l). However, the medical records released by the covered entity must be limited to the minimum-necessary requirement.

The amount of minimumly necessary information is determined by reference to the applicable state Workers' Compensation law. The statutory scheme may

create problems in some states where the practice on obtaining medical records is more generous than the statutory language. For example, consider the current law and practice in Arkansas:

Statute: Ark. Code Ann. § 11-9-516 provides:

Every hospital or other person furnishing the injured employee with medical services shall permit its records to be copies and shall furnish full written information to the Workers' Compensation Commission, the Workers Compensation Fraud Investigation Unit, the employer, the carrier, and the employee or the employee's dependents.

(Creates minimum necessary cap – records of providers of treatment for current claim.)

Regulation: Ark. WCC Rule 30, Part VI(B) provides:

Health care providers and facilities must furnish an injured employee or his attorney and carriers/self-insureds or their attorneys copies of his records and reports upon request. The charge shall be the same as set out in Ark. Code Ann. § 16-46-106(a)(2).

(Creates same minimum necessary problem on the statute.)

Workers' Compensation Forms: The practice in Arkansas is that employers and Workers' Comp carriers can obtain the entire medical record on a claimant including pre-existing and unrelated treatment. The authorization for this is found in Form AR-C and Form AR-N as follows:

I hereby authorize any hospital, physician, psychotherapist or practitioner of the healing arts to furnish the bearer any information, written or oral, including, but not limited to, copies of medical records concerning my past, present or future physical, mental or emotional condition. I hereby waive my physician – and psychotherapist-patient privilege. A photostatic copy of this authorization shall be as effective and valid as the original.

(Eliminates minimum necessary, but would not meet requirements of a valid HIPAA authorization.)

Considering that health care providers could be subject to fines and criminal penalties for a violation of HIPAA, they may take a more restrictive view of what is minimally necessary than the carrier. In this case the provider can still get the medical record considered necessary by using a HIPAA compliant authorization.

APPENDIX

Following are some useful websites for HIPAA research:

http://www.hhs.gov/ocr/hipaa

http://www.gpoaccess.gov/index.html

http://aspe.hhs.gov

http://www.gpoaccess.gov/cfr/index.html

http://www.gpoaccess.gov/fr/index.html

http://www.hipaa.org/

http://www.cms.hhs.gov/hipaa/hipaa2/default.asp?

