

Healthcare News

An occasional communication offering operational insights for physicians, medical practices, and other employers.

Employer-Sponsored Group Health Plans & HIPAA's Third Installment

by: Laura Gerdes Long (llong@dmfirm.com)

If small business employers think that the Health Insurance Portability and Accountability Act—or what we fondly refer to as “HIPAA”—only applies to health care providers, they need to think again. Small business owners need to get hip to HIPAA because those that offer employer-sponsored health plans (as most do) must also protect the privacy of employees’ medical information.

Physician practices typically understand they are “Covered Entities” under HIPAA due to their status as medical providers but many are unaware they may carry the title of “Covered Entity” by way of their employer status.

Though employers are not Covered Entities under HIPAA, many employers offer fully or partially self-funded health plans to their employees and *those health plans are Covered Entities under HIPAA*. Indeed, even flexible spending accounts or 125 plans are considered health plans and thereby must comply with HIPAA.

Last April, the final installment in the series of three HIPAA regulations went into effect. The first installment was the Electronic Health Care Transaction and Code Sets (October 2002). The second installment was the Privacy Rule (April 2003 or April 2004 for small group health plans). Finally, as of April 20, 2005, all covered entities (as defined by HIPAA) were required to implement the Security Rule. Small health plans, defined as those that spend \$5 million or less in claims, were given until April 20, 2006, to comply.

The Security Rule, a series of standards, provides administrative, physical and technical safeguards to protect the security of electronic health information. It may be found at Title 45, Code of Federal Regulations, Part 164, Sections 302-318 (45 CFR 164.302).

While the Privacy Rule includes a mini-security rule, the regulations of the Security Rule are far more detailed and include comprehensive ways in which a covered entity may

perform a risk analysis to determine the measures required to comply with the Rule. The Security Rule applies to the same covered entities as the Privacy Rule and similarly applies to the covered entities’ business associates. If you offer a health plan to your employees, that plan must meet both the Privacy Rule and Security Rule requirements. By extension, the employer must ensure that the plan has met those requirements.

For small plans, compliance may be simple, especially when most employers outsource their health care operations to third party administrators and have very little interaction with electronic protected health information, or PHI.

Like the Privacy Rule, the Security Rule requires health plans to limit disclosures of PHI to the plan sponsor employers unless certain conditions are met. Consequently, non-covered entity employers who are health plan sponsors are affected by HIPAA’s Security Rule including having to amend employer health plan documents to incorporate provisions requiring such employers who receive PHI from the health plan to implement security safeguards.

These safeguards include three standards which fall under the categories of administrative, physical and technical, and numerous implementation specifications.

In this issue...

- ◆ The Mental Health Practitioner—page 2
- ◆ Personnel Records: What Goes Where—page 4
- ◆ Physician Practices & Records Transfer—page 5
- ◆ Recent Cases Involving Patient Privacy—page 6

The good news is that the Security Rule permits flexibility in your entity's approach based upon organizational size, complexity, staff capabilities, the likelihood of potential risks, costs, and your computer hardware and software capability.

It's also a good time to be reminded that every three years, covered entities should revisit their adherence to the Privacy Rule requirements by evaluating actions taken and determining whether it is appropriate to modify compliance processes and procedures. HIPAA compliance does not have a completion date, rather it is an ongoing process. ◇

The Mental Health Practitioner—HIPAA—Psychotherapy Notes

by: Guest author, Daniel P. Card, II (dcard@lawyer.com)

In *Jaffee v. Redmond*¹ the U.S. Supreme Court in a landmark, pre-HIPAA decision, held that federal courts are to recognize and apply a psychotherapist-patient privilege.² To this the Court commented:

Like the spousal and attorney-client privileges, the psychotherapist-patient privilege is "rooted in the imperative need for confidence and trust." Treatment by a physician for physical ailments can often proceed successfully on the basis of a physical examination, objective information supplied by the patient, and the results of diagnostic tests. Effective psychotherapy, by contrast, depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. Because of the sensitive nature of the problems for which individuals consult psychotherapists, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason, the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment.

.... The psychotherapist privilege serves the public interest by facilitating the provision of appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance.

Missouri State Law

Unfortunately, despite the heightened sensitivity and reasons justifying the privacy of mental health records, some outsider will most likely be able to obtain copies of a patient's mental health records. The reasons vary and include: (1) by consent, via a signed patient authorization; or (2) the patient's participation in litigation where his/her mental health is at issue—whether the claim is for personal injuries, mal-

practice, employment discrimination, emotional stress, or even child custody litigation.³

However in Missouri, as with most states, a waiver of the psychotherapist-patient privilege is oftentimes an all or nothing proposition. Usually, the person seeking such records will be able to see all or none of the records. Such disclosure may include materials which many mental health practitioners consider to be the most sensitive and private including the contents of private or group counseling sessions, patient disclosures, patient statements, and/or a therapist's impressions. These materials have historically been referred to as either "process notes" or "personal notes."

Illinois law, however, provides protection of these personal notes. The Illinois Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS §110/3(b) provides:

A therapist is not required to but may, to the extent he determines it necessary and appropriate, keep personal notes regarding a recipient. Such personal notes are the work product and personal property of the therapist and shall not be subject to discovery in any judicial, administrative or legislative proceeding or any proceeding preliminary thereto.

Personal notes under the Illinois statute are defined as:

- (i) information disclosed to the therapist in confidence by other persons on condition that such information would never be disclosed to the recipient or other persons;
- (ii) information disclosed to the therapist by the recipient which would be injurious to the recipient's relationships to other persons; and
- (iii) the therapist's speculations, impressions, hunches, and reminders.

In Missouri, no comparable provision exists. As a result, some Missouri practitioners have informally, but without official sanction by either statute or administrative regulation, adopted a “dual record-keeping” practice. In this way, the practitioner has an “official file” and a separate “private file.” The latter file is one they would not disclose or make reference to even upon receipt of a subpoena, court order, or properly signed authorization.

Health Insurance Portability and Accountability Act

In its final HIPAA privacy regulations, the U.S. Department of Health and Human Services (“HHS”) addressed, at least in part, the need for “psychotherapy notes to be accorded a heightened level of privacy protection.”⁴ However, the heightened level of privacy which the HIPAA regulations accord to “psychotherapy notes” is not without exception.⁵

What are psychotherapy notes under HIPAA? What records are excluded? What are the advantages and/or the disadvantages of keeping and employing in one’s practice separate psychotherapy notes?

Whether one chooses to keep and use separate psychotherapy notes in one’s practice is a subject with which mental health professionals should be thoroughly familiar.

The HIPAA Privacy Rule defines psychotherapy notes as:

... notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session **and that are separated from the rest of the individual’s medical record.** (emphasis supplied).

HIPAA’s definition of psychotherapy notes, however, specifically **excludes** certain records, as follows:⁶

Psychotherapy notes excludes medication prescription and monitoring, counseling session start up and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Accordingly, under the HIPAA privacy regulations, it is apparent that psychotherapy notes that have been properly identified and kept separate from the rest of the patient’s file should receive a heightened level of privacy.

Of course, records identified and kept separately as psychotherapy notes must be strictly limited in order to qualify them as such. Psychotherapy notes, if commingled with other, non-psychotherapy note information would probably not be afforded this protection. Thus, progress notes under the HIPAA definition are not the same as psychotherapy notes.

Finally, the heightened right of privacy given to psychotherapy notes under HIPAA has several components. First, the health care provider generally must obtain from the patient a specific, signed authorization for the release of the psychotherapy notes. This authorization must be separate and distinct from a general authorization.

Second, absent a signed patient authorization, a health care provider is limited in how and to whom the psychotherapy notes may be used or disclosed. As a general rule, a covered entity must obtain a signed authorization for the disclosure of the psychotherapy notes to anyone, except to disclose or use the records to carry out treatment, payment or health care operations, to the creator of the notes for treatment, for internal training programs, and/or to allow the provider to defend himself from legal actions instituted by the patient against the provider.

Accordingly, if the requester does not have a specific, signed authorization, then psychotherapy notes may only be disclosed or used where the disclosure is: (1) required for enforcement purposes; (2) mandated by law; (3) for judicial or administrative proceedings; (4) required by a health oversight agency; (5) needed by a coroner or medical examiner; and/or (6) required to avert a serious and imminent threat to the health or safety of a person or the public. It is important to note, however, that HIPAA may impose additional limitations and/or procedures which must be followed, even under these exceptions.

Third, a health insurer or health plan may not condition the enrollment, eligibility for benefits, or payment of a claim on obtaining the patient’s authorization to obtain psychotherapy notes.

Fourth, although generally a patient has the right to obtain access to his/her own medical records, a health care provider may decline to release or disclose psychotherapy notes to the patient himself.

Conclusion

Because Missouri does not have more stringent laws protecting the privacy of patient records with respect to psychotherapy notes, HIPAA provides the guiding principles for health care professionals in this area. Hence, as part of their HIPAA compliance review, a mental health practitioner would be well advised to examine record keeping practices and restructure where needed. ♦

¹ 518 U.S. 1,10 (1996).

²In Missouri, the psychotherapist/patient privileges are creatures of statute.

³State ex rel. McNutt V Keet, 432 S.W.2d 597, 601 (Mo. banc 1968); State ex rel. Stecher v. Dowd, 912 S.W.2d 462, 464 (Mo. banc 1995); State ex rel. Dean v. Cunningham, 182 S.W.3d 561, 567 (Mo. banc 2006) (emotional distress); Seyler v. Seyler, 201 S.W.3d 57, 63 (Mo. App. E.D. 2006) (child custody).

⁴The American Psychological Association (“APA”) submitted comments on both the proposed and final HIPAA privacy regulations wherein it strongly advocated that “heightened protection” should be accorded to “psychotherapy notes.” See, Jones, Held to a Higher Standard, APA ONLINE (2006). HHS, however, adopt rejected the APA’s suggestion that the regulations broaden the phrase “psychotherapy notes” to include psychological test data and test material.

⁵In this regard, however, it is important to note that the HIPAA privacy regulations only preempt state laws which are less stringent and/or provide less privacy protection. Therefore, if a state law is more stringent than a HIPAA provision, than health care providers, including mental health practitioners, are still bound by those stringent state laws. See 45 C.F.R. §160.203.

⁶HHS’s stated rationale was that, “[a]lthough all psychotherapy information may be considered sensitive, we have limited the definition of psychotherapy notes to only that information that is kept separate by the provider for his or her own purposes.”

Personnel Records: What Goes Where

by: Laura Gerdes Long (llong@dmfirm.com)

Confusion abounds when it comes to deciding which employee personnel records go where, who can access which records and who cannot, and how records should be segregated. Human resource employees have long understood that an employee’s workers’ compensation records should be segregated from the employee’s typical personnel file containing such things as an application for employment, resume and salary change forms.

For the small employer, however, these kinds of decisions must be addressed by management, who may not always be experienced in the nuances of human resource law.

In essence, three files should be maintained for each employee:

1. The **personnel** file contains new hire and termination information, change forms, performance documentation and miscellaneous information such as requests to inspect employee files, underemployment claims, training courses, and achievements.
2. The **confidential** file contains information such as references, background investigations, financial obligations, settlement agreements, and EEO data.

Information not specifically related to employee wage and hour status or job performance should be scrutinized to determine whether it reveals any private facts about an individual. If it does, it should be placed in this file rather than the Personnel File. This could include:

- ♦ health-related documentation (not related to the health plan), e.g., injury reports, requests for reasonable accommodation, FMLA forms, fitness for duty, post-offer medical information, workers’ compensation injury forms and reports, disability leave documentation, and self-identification of disability;
 - ♦ financial information, including W-4’s (federal and state), direct deposit authorization, payroll corrections, requests for verification of employment, wage attachments, credit reports, and retiree insurance premium agreements; and
 - ♦ miscellaneous information, including settlement, arbitration and dispute agreements and decisions; EEO complaints or other information; investigation interview notes; grievances; affirmative action; reference and background check forms; interview evaluation, skills or personality tests, funeral and jury duty notices.
3. The **Confidential Protected Health Information** (“PHI”) file, includes all the information pertaining to the health plan(s) offered by the employer, including, self-insured health plans, flexible spending accounts (for medical and prescription) and cafeteria plans:
 - ♦ benefits enrollment forms;
 - ♦ benefits change forms;
 - ♦ benefits claim forms;

- ◆ dependent and beneficiary designations;
- ◆ insurance waivers;
- ◆ open enrollment forms;
- ◆ COBRA documentation;
- ◆ health care provider certification;
- ◆ voluntary medical information; and
- ◆ authorization to release information (pre-employment).

Drug and alcohol tests should be filed in a separate binder, not with any other information, segregated by current and separated status. Form I-9's should also be filed in a separate binder, segregated by current and separated status. ◆

Physician Practices and Records Transfer in the HIPAA Era

by: Laura Gerdes Long (llong@dmfirm.com)

In the current environment, it seems that businesses are constantly changing hands, merging or dissolving. The question then is what happens with a patient's medical records when a medically-based business is bought, sold or dissolved? State laws and HIPAA inform the answer.

In Missouri, patient records under the care, custody and control of a medical licensee must be maintained for a minimum of seven years from the date of when the last professional service was provided. (R.S.Mo. § 334.097).

If selling a practice, a series of steps must be accomplished when notifying patients of the sale, including notifying the patient of the process for obtaining a copy of medical records and the potential need for the written authorization before medical records can be transferred to another provider. Moreover, under HIPAA, a specific authorization is required for the release of information considered sensitive, such as HIV/AIDS status, psychiatric history, drug or alcohol abuse, or sexual abuse.

Since the *physical* record is considered the property of the practice and the *information in* the record is considered the property of the patient, a practitioner who is leaving one practice to go to another should not simply take the records with him of those patients who will continue in his or her care.

For instance, if a practice is dissolved, a custodian of patient records may have to be located and a business associate agreement obtained requiring that custodian or receiving physician to respect the confidentiality of the records in accordance with HIPAA. The state medical board or department of health should also be notified where the records are

being stored in case patients, at some point in the future, need to access their records if the former physician or custodian cannot be located.

In addition, the Code of Ethics of the American Medical Association at E-7.03 provides similarly. Patients should initially be notified and informed that upon authorization, their records will be sent to their choice of physician. Any records not forwarded to a new physician should be retained, either by the treating physician, another physician, or such other person lawfully permitted to act as a custodian of the records. If the physician is leaving a group practice, after notification, the patients should also be informed of the physician's new address and offered the opportunity to have their medical records forwarded to the departing physician at his or her new practice location. The Code warns that it is unethical to withhold such information upon request of a patient.

In the case of a retiring physician, it may be most practical to transfer the records to a hospital. The hospital should agree to treat the records as if they were their own for HIPAA purposes and only transfer the records to another physician upon the patient's written authorization. Essentially, the hospital becomes a business associate of the retiring physician and is subject to the business associate requirements of HIPAA.

As you can see, many issues and precautions must be taken into account when a physician retires, moves from an existing practice, or sells a practice with regard to patient records. ◆

Recent Cases Involving Patient Privacy—How Far Does the Duty Go for Employees?

by: Laura Gerdes Long (llong@dmfirm.com)

On May 24, 2006, the Illinois Supreme Court granted an appeal for a defendant hospital's petition for leave. A decision in this case* concerns the extent of an employer's liability for an employee's off-site and off-duty breach of a patient's privacy.

The case alleged that plaintiff was a patient at a particular medical group. Blood samples and/or records were sent to a hospital and examined by a phlebotomist. The phlebotomist revealed the results of those records at a public tavern to the plaintiff's twin sister. The hospital admitted the phlebotomist had revealed one fact about the plaintiff, discovered from her medical records, to the plaintiff's sister at a tavern, but also alleged that when the phlebotomist revealed the information, she was not acting within the scope of her employment with hospital. Although HIPAA does not provide a private cause of action, in Illinois a common-law right-of-privacy cause of action existed for the doctor's violation of plaintiff's right to privacy.

The court held that the question whether the phlebotomist was acting in the scope of her employment with the hospital was a question for the jury. The court went on to note, however, that the defendant hospital and employee had a duty not to disclose confidential information, without limitation as to time or place.

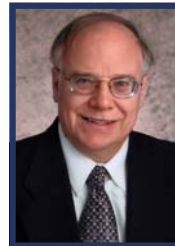
The court reasoned that the "hospital's training of its employees did not limit the duty of the employee to maintain confidentiality of patients' medical information only during working hours. Rather, that duty, imposed by the hospital in its execution of its duties, was, according to its own training, to extend to all times and to all places. In effect, for purposes of patient confidentiality, [the phlebotomist] was on duty 24 hours a day, 7 days a week." Thus, the defendant had a continuing off-shift duty to maintain the confidentiality of patient records. This duty derived not only from the hospital's rules of employment, but also from the patient's right to privacy.

The court further included employees of lawyers, therapists, and other employers who maintain confidential information, as examples of other workers who have a constant duty to keep confidentiality. ♦

**Bagent v. Blessing Care Corporation, d/b/a Illini Community Hospital, 844 N.E.2d 469 (Ill.App. 4th Dist. 2006).*

Our Healthcare Practice Group:

- ♦ Michael McKitrick
- ♦ Cheryl Beebe-Snell
- ♦ Ruth Binger
- ♦ Laura Gerdes Long
- ♦ Sophya Qureshi
- ♦ Jeffrey Schmitt



Daniel P. Card, a principal with Family Law Group, LLC, consults with healthcare professionals regarding professional licensure, ethical investigations, confidentiality, privilege, HIPAA, duty-to-warn, conflicts of interest, and impermissible dual relationships. Dan serves as a lecturer, seminar, and CE presenter.

Questions? Call 314.726.1000

www.dannamckitrick.com

150 N. Meramec, Fourth Floor
St. Louis, MO 63105



Laura Gerdes Long litigates and consults on employment, tort, insurance, municipal, healthcare, and professional liability matters. Proficient in employment law policies and processes related to HIPAA, she serves in the role of trainer and advisor to self-insured employers, municipalities and fire districts.