Silent PPOs Must Be Heard: States Increasingly Require Disclosure

Health plan, insurer, and preferred provider organization (PPO) provider agreements typically incorporate language extending contractual benefits to “other payors.” Such sale, leasing, or transfer arrangements permit third parties to access the contracting entity’s provider network and, with it, negotiated provider discounts. (Third parties at times include worker’s compensation insurers and self-funded employer groups.) In response to objections to undisclosed or “silent” PPOs created by such arrangements, states have enacted laws regulating their use.

Such legislation generally requires contracting entities to make certain disclosures upon entering and renewing a provider contract. In California, for example, prohibitions on silent PPOs require extensive disclosures by contracting entities, including whether its provider list may be sold or otherwise conveyed, how it actively promotes steerage to network providers, and which payors are eligible to claim a provider’s contracted rate. The statutory scheme requires “other payors” claiming the discount to actively promote network providers in their directories and other communications and to identify in the explanation of benefits forms the plan or network that has a written contract signed by the provider pursuant to which the payor is entitled to pay a preferred rate. Recent statutory amendments preclude transfer of only the provider discount; the “other payor” is held to the same obligations, including benefit packages and payment rules, set forth in the underlying provider agreement.

Under Texas law, insurers or administrators cannot reimburse a preferred provider at the negotiated rate unless they have a contract with that provider, nor can such entities sell, lease or transfer information regarding reimbursement terms absent the provider’s consent. A legislative amendment to enact comparable restrictions is pending in Florida. In Louisiana, PPO alternative rates of payment are unenforceable against any provider unless the accessing entity is clearly identified on the patient’s healthcare benefit card. North Carolina has gone so far as to define a silent PPO as an unfair trade practice. To date, some 14 states have enacted laws regulating their use.

In contrast to the plethora of legislative solutions, few silent PPO challenges have found their way to the courts. One such case, HCA Health Services of Georgia, Inc. v. Employers Health Insurance Co., 240 F.3d 982 (11th Cir. 2001), held that a silent PPO agreement violated ERISA by depriving beneficiaries of their legitimate expectation of higher payments to out-of-network providers. The court concluded that the discount was neither permitted by the terms of the agreement between the beneficiary’s health plan and the insurance company payor, nor the provider’s contract with the PPO that thereafter conveyed the discount to the payor. In another case, New England Physical Therapy Network, P.C. v. Healthcare Value Management, Inc., 2002 WL 1923805 (Mass. Super.), defendants were alleged to have “misappropriated ... preferred provider organization discounts.” More recently, in Coy v. Country Mut. Ins. Co., 2006 WL 3487653 (S.D. Ill.) (alleging the taking of discounts without steerage) and Komeshak v. Risk Enterprise Management Services, Inc. 2006 WL
3147703 (S.D. Ill., 2006) (alleging “improper ‘silent PPO’ discounts”), the cases were decided on unrelated procedural grounds, without addressing the underlying “silent PPO” issues presented.

These issues appropriately should be handled early on during contracting. Health plans, insurers, PPOs and other contracting entities should inventory their network leasing provisions to ensure that they are not vulnerable to provider attack due to imprecise drafting. They also should undertake periodic review to ensure compliance with mandated disclosures and other obligations. Providers should fully analyze the payor and product provisions of proposed contracts to ascertain their financial impact before signing. Together with protective legislation, these efforts should go a long way toward eliminating any adverse consequences of silent PPOs and minimize the need for litigation.

- Submitted by Shelley Hubner
Sedgwick San Francisco

Who’s Liable When Private Data Is Improperly Disclosed?

Improper disclosure of a patient’s personal and/or medical information can occur in unique situations. Two recent cases, neither involving improper computer disclosure, are instructive on how courts are being asked to expand legal duties beyond traditional boundaries. (See related article on security breaches and implications for healthcare providers on page 3 of this newsletter.)

In Suzanne Bagent v. Blessing Care Corp., d/b/a Illini Community Hospital, et al., __ N.E. 2d ___, 2007 WL 121319 (Ill 2007) (not yet released for publication), the Illinois Supreme Court found that a hospital employee’s improper disclosure of confidential information about a patient did not expose the hospital to liability under a theory of respondeat superior. In that case, the hospital employee’s actions, while she was off duty in a tavern, were not found to be within the scope of her employment.

In Bagent, the patient sued not only the hospital but also the hospital’s employee, Misty Young. Young improperly disclosed medical information about Bagent at a bar. As a phlebotomist (a person who draws blood) for the hospital, Young attended a hospital training session, which included information about the Health Insurance Portability and Accountability Act (HIPAA) and the necessity to comply with its privacy provisions. Young also signed the hospital’s confidentiality policy and code of conduct and received what the hospital referred to as a “motto to remember”: “What you see here, and what you hear here, remains here.”

As part of her job, Young received a fax communication from a facility that performed blood tests for patients of the hospital. The fax revealed that a patient, Bagent, had a positive pregnancy test. Young had an obligation to keep information learned at her job private.

Young went to a bar a few days later. As circumstances would have it, the plaintiff’s sister was one of Young’s best friends. During the course of her conversations with the plaintiff’s sister, Young disclosed that she knew Bagent was pregnant. When the hospital learned of the conversation that took place at the bar, it advised Young she could resign or would be terminated. Young accepted the hospital’s offer to resign.

Plaintiff Bagent then filed suit against the hospital and Young alleging the following causes of action:

• Breach of healthcare practitioner/patient confidentiality;
• Invasion of privacy;
• Negligent infliction of emotional distress; and
• Intentional infliction of emotional distress (against Young only).

All causes of action were alleged violations of the Illinois Hospital Licensing Act, the Illinois Managed Care Reform and Patients Rights Act, and the Illinois Constitution.

In its answer, the hospital admitted that Young had disclosed confidential information. It argued that the disclosure was made at a time when Young was acting outside the scope of her employment with the hospital. It also argued that neither the Illinois Constitution nor the state statutes referenced above created a private right of action.

The trial court granted summary judgment in favor of the hospital on the statutory claims, finding the statutes did not create a private cause of action. The trial court also granted summary judgment to the hospital on the right to privacy claims, holding that Young’s disclosures were not made within the course or scope of her employment. The
appellate court then reversed. It found a genuine issue of material fact existed concerning whether Young’s disclosure was motivated, in part, by a purpose to serve the hospital.

On further appeal, the Illinois Supreme Court reversed and upheld the trial court’s rulings. The Supreme Court found merit to the hospital’s argument that the disclosure of a patient’s condition in a conversation off premises was not the kind of conduct the employee was employed to perform. The hospital's affirmative actions, including training sessions and its confidentiality policy, were cited by the court in support of its conclusion that the conduct was not within the scope of employment but was specifically prohibited.

In another case involving improper disclosure of information to a third person, a North Carolina appellate court was asked to address whether a patient’s negligence claim for improper disclosure of information could be based on alleged violations of a hospital’s rules and regulations and HIPAA.

In Acosta v. Byrum, 638 SE 2d 246 (NC App. 2006), a patient sued her psychiatrist, and others, alleging negligent infliction of emotional distress. Acosta was both a patient and employee of the defendant psychiatrist’s practice group (Psychiatric Associates of Eastern Carolina). Acosta and the office manager, Robin Byrum, did not get along. In fact, plaintiff contended that Byrum had severe personal animus toward her. Over 10 months, the owner of the practice, Dr. Faber, allowed Byrum to use his personal access number to get access to plaintiff’s confidential psychiatric and medical records. Byrum then provided information found in those records to third parties without plaintiff’s authorization or consent. Plaintiff alleged this conduct violated the duties created under the hospital’s rules and regulations and under HIPAA. She also contended these alleged violations were sufficient to form the basis of her negligent infliction of emotional distress claim.

The trial court granted the physician’s motion to dismiss finding that plaintiff had not sufficiently alleged a negligence claim. The appellate court reversed, finding that plaintiff’s reference to general rules and regulations of the hospital and HIPAA without citing specific provisions was enough to put the physician “on notice” as to how plaintiff intended to establish the alleged duty to maintain privacy in her confidential medical records. While HIPAA does not create a private cause of action, the appellate court concluded that the plaintiff was entitled to rely on the statute as a basis for establishing the standard of care for her common law negligence claim.

Given the ever-expanding access to medical records, opportunities for the improper disclosure of protected medical information are endless. So too will be the litigation that follows. Bagent and Acosta are examples of the creative ways in which injured parties will seek redress in the courts for their alleged injuries. As noted by the Illinois Supreme Court in Bagent, proper training of employees on confidentiality issues and establishment of policies and procedures in this area will be crucial to the defense in future litigation involving privacy issues.

- Submitted by Carol J. Gerner and Fred A. Smith, Sedgwick Chicago

Court Holds Maryland’s ‘Wal-Mart’ Law Preempted by ERISA

In Retail Industry Leaders Ass’n v. Fielder, ___F.3d___; 2007 WL 102157, C.A.4 (Md.), January 17, 2007 (NO. 06-1840, 06-1901), the U.S. Court of Appeals for the Fourth Circuit affirmed a Maryland district court’s decision holding that the Maryland “Fair Share Health Care Fund Act” is preempted by ERISA and therefore unenforceable. The Maryland law in question, also known as the “Wal-Mart Law,” required large employers in the state to devote at least 8% of total wages paid to employees in the state to health insurance costs for its employees, or pay the difference between what is spent on employee health insurance and 8% of wages to the state. In turn, any money paid to the state under this law would be earmarked exclusively for state Medicaid or children’s healthcare purposes.

The Fourth Circuit affirmed, in a 2-1 decision, that the law is preempted by ERISA because it mandates the structure of health benefit plans by requiring employers to fund their plans in accordance with a predetermined formula and to meet a minimum spending threshold. Although Maryland’s Secretary of Labor, Licensing & Regulation argued that the law did not relate to the administration of ERISA plans because it gave
employers affected by the law the option to either pay the state the additional amount of money required or to increase health insurance spending on non-ERISA type plans (such as HSA contributions or on-site medical clinics), the Fourth Circuit disagreed. The court ruled funding non-ERISA healthcare options would likely not make up the difference in health care dollars spent and that no reasonable employer would pay money to the state if it could spend it on benefits for its own employees. In effect, the practical result of the law would require large employers in the state to provide a mandated level of employee health benefit funding, in violation of ERISA rules that do not require any employer to provide such benefits or mandate the level of benefits when they are provided.

The Fourth Circuit also held that the Maryland law, and others like it, interfered with ERISA’s goal of uniform national plan administration because it could expose large employers to differing state and local laws concerning plan funding. The court specifically noted that other state and local governments had passed similar laws requiring large employers, specifically Wal-Mart, to spend a predetermined amount on healthcare for its employees in these various localities. The Fourth Circuit found that the Maryland act clashed with the spending mandates set forth in these other state and local laws. The court specifically noted that two New York counties had already passed such laws and that similar legislation is being considered in Minnesota. The Fourth Circuit concluded that if such laws are permitted to stand, large national employers such as Wal-Mart will be left with the daunting task of attempting compliance with a patchwork of different rules and requirements from state to state, or even from county to county. “This is precisely the regulatory balkanization that Congress sought to avoid by enacting ERISA’s preemption provision,” the court wrote.

- Submitted by Mike Bernstein
  Sedgwick New York

HIPAA Does Not Provide Right of Action in Privacy Violation Cases

The Health Insurance Portability and Accountability Act (HIPAA) serves as the basis for the development of privacy regulations that health care providers have been implementing since its enactment. HIPAA does not contain any express language conferring rights upon a specific class of individuals if the privacy regulations are violated. Instead, it focuses on regulating persons who have access to individually identifiable medical information and who conduct certain electronic health care transactions. HIPAA provides both civil and criminal penalties for improper disclosure of medical information. Notwithstanding the importance of safeguarding patient’s personal healthcare information, the act does not afford a private right of action. A recent decision by the Fifth U.S. Circuit Court of Appeals, Acara v Banks, 470 F.3d 569 (5th Circuit CA, 2006), is the first of many appellate decisions likely to follow upholding a district court decision that HIPAA does not afford a private right of action.

In Acara, a patient filed suit in federal court against her physician for disclosing her medical information during a deposition without her consent. By filing in federal court, Acara attempted to use HIPAA as the basis for federal court jurisdiction. The decision did not address the reasons why the disclosure of the medical information was improper in the context of the physician’s deposition. If, for example, Acara’s medical condition was at issue, the defense attorney for the physician should have obtained and/or followed a court order governing whether Acara’s medical condition and health records could have been discussed. Alternatively, the attorney could have sought an appropriate waiver from Acara before the deposition. Because the court focused only on the question of federal jurisdiction, it did not delve into any of these concerns. It just ruled there was no private right of action under HIPAA.

While HIPAA may not serve as a basis for a private right of action, the privacy concerns that prompted its enactment may nonetheless need to be addressed for matters in litigation as noted above. They also need to be addressed to the extent they are used as the basis for alleging a standard of care in a common law negligence action for breach of privacy. (See article on the recent North Carolina appellate decision, Acosta v Byrum, in this newsletter on page 3.)

The statutory language in HIPAA appears to limit enforcement of the statute to the Secretary of Health and Human Services. However, certain alleged HIPAA violations and concerns over privacy of protected health information may also trigger state attorney general investigations.
According to news reports, Westerly Hospital in Rhode Island found itself the victim of a security breach involving the posting on the Internet of a “snapshot” of patient interactions (called a face sheet) for 2,242 of its patients. The information was made available on an Internet site hosted by Yahoo. The posted information contained the patient’s name, contact information, insurance policy numbers, and in many cases, the patient’s social security number. None of the patient’s actual medical record was disclosed. The hospital maintains that it complied with HIPAA and state law. The hospital also contends that it had no reason to believe that the hospital’s computer security measures failed.

The Rhode Island attorney general is investigating to try to determine who posted the information and whether any hospital officials were aware of the security breach before a patient called the local police. At this time, it is unknown how the information was obtained, who posted it, who viewed the information online or how long it had been posted before being discovered and dismantled several hours later.

The hospital is taking measures to notify patients and has offered to provide credit protection for those affected. It is also working with local authorities. Once the hospital was made aware of the posting, it contacted the Rhode Island Department of Health, the Rhode Island Attorney General’s office, the U.S. Attorney General’s Office, major insurers in the area, the Joint Commission, and the Centers for Medicare and Medicaid Services. It also brought in an outside computer security firm to work with its own internal IT department.

The fact that the Rhode Island attorney general is investigating this security breach is noteworthy. Last month, the Rhode Island attorney general filed a civil investigative demand (CID) against TJX, the parent company of stores such as TJMaxx. In the CID, the attorney general alleged that by allowing a security breach on its computer network, TJX violated Rhode Island’s Deceptive Trade Practices Act. In that incident, TJX learned of the breach in December but did not disclose it until January. The attorney general disagreed with TJX’s position that delay in making the announcement enabled it to contain the problem and further strengthen its computer network to prevent further intrusion. Based on the position of the Rhode Island attorney general in the TJX case, the issue of notice of the security breach and the timing of the disclosure may be of great importance, including whether further governmental action will be initiated and under what authority.

-Tenth Circuit Holds Claimant Not Entitled to Comment on Medical Report Prepared at Appeal Level

In Metzger v. Unum Life Insurance Co., No. 06-3064, __ F.3d __, 2007 WL 521226 (10th Cir. Feb. 21, 2007), the Tenth U.S. Circuit Court of Appeal held that claims administrator UNUM Life Insurance Co. of America did not need to provide an opportunity to the claimant to comment on medical reports prepared during the administrative appeal prior to the issuance of UNUM’s final decision.

On appeal to the Tenth Circuit, the claimant asserted that UNUM failed to provide her with a “full and fair” review due to UNUM’s unwillingness to provide the reports before the final decision. The claimant relied on 29 C.F.R. §2560.503-1(h)(2)(iii), which requires disclosure of “all documents, records and other information relevant to the claimant’s claim for benefits.” The district court noted that if the claimant were given the opportunity to comment on every medical opinion generated on appeal, it would create an “endless loop of opinions.” The Tenth Circuit agreed with the district court’s reasoning, holding that the regulations do not require an “administrator to provide a claimant with access to the medical opinion reports of appeal-level reviewers prior to a final decision on appeal.”

In reaching this conclusion, the court’s view was most likely shaded by the elevator ride of appeals and remands between the administrator, district court and court of appeals. UNUM initially denied the claim and upheld the decision because it did not appear that the claimant was under the regular care of a doctor and she was not disabled under the terms of the employee benefit plan. In reaching its final decision, UNUM relied upon two medical reports prepared during the appeal.

The claimant commenced the initial lawsuit challenging UNUM’s final decision to deny her disability benefits and sought an opportunity to address
the medical reports. The district court remanded the matter to UNUM to allow that opportunity. On remand, the claimant submitted additional materials, and UNUM sent the entire file to a board certified physician and a vocational consultant. Both concluded that the claim should be denied. UNUM again upheld its decision to deny disability benefits and refused to provide the new medical reports before the final decision.

The district court revisited its initial decision, allowing the claimant to comment on the medical reports, and reached the opposite conclusion. The district court held that UNUM did not have to provide an opportunity to the claimant to comment on those reports prepared at the appeal level.

The Tenth Circuit agreed. In doing so, it disagreed with *Abram v. Cargill, Inc.*, 395 F.3d 882 (8th Cir. 2005), which found that the claimant was entitled to an opportunity to comment on the medical report prepared at the appeal level before the final decision. The Tenth Circuit limited *Abram* to a decision interpreting the disclosure regulations in effect in 2000, and not the new regulations in effect today, noting that the *Abram* court did not consider the “potential for circularity of review.”

- Submitted by John T. Seybert
  Sedgwick New York

**Sedgwick Healthcare Attorneys**

**Serving the Legal Community**

San Francisco Special Counsel Shelley Hubner was appointed to the ABA’s Governing Council of its Health Law Section. In this role, Ms. Hubner will assist the group in its mission to increase interest in health law through innovative educational and service programs.

New York Partner Mike Bernstein was selected to continue as chair of the Defense Research Institute Life, Health and Disability Committee’s Web site subcommittee.

Los Angeles Partner David M. Humiston was nominated and elected a Fellow of the American Bar Association.

**Articles**

“*You Can’t Get There From Here -- ERISA Preemption of State Laws Mandating Employer Healthcare Contributions*”

By Mike Bernstein and John Seybert

*ABA Health eSource*

March 2007

“*Ninth Circuit Effects Sea Change In ERISA Discretionary Review*”

By Dennis G. Rolstad

*Employment Law360*

December 6, 2006

“The Impact of Silent PPOs on the Managed Healthcare System”

By Fred Smith and Bob Bohner

*Healthcare Liability & Litigation (Published by the American Health Lawyers Association)*

Fall 2006

“*Court Rules That Provider Underpayment Claims Against HMO Are Preempted by ERISA*”

By Mike Bernstein

*DRI ERISA Report* (published by the Defense Research Institute)

September 12, 2006

---

© 2007 Sedgwick, Detert, Moran & Arnold LLP