ReedSmith

Health Law Monitor

Spring 2007

Volume XI, Number 1

How to Prevent (or Respond to) a Data Security Breach and Identity Theft

A data security breach is something all health care entities try to avoid. Inadvertent disclosures of personal or other confidential information caused by a breakdown in security expose health care entities to a host of liabilities (under both federal and state law). In addition, a security breach may mar a health care entity's reputation and lead to a loss of consumer confidence. Most health care providers (such as hospitals and nursing homes) and health insurers have invested significant resources to protect the privacy and security of patient health information in response to HIPAA (Health Insurance Portability and Accountability Act of 1996). However, health care providers, as well as other types of health care entities that may not be directly covered by HIPAA (such as pharmaceutical and device manufacturers and group purchasing organizations), also maintain information that is just as sensitive, but is not protected by HIPAA. This information may not fall within an entity's existing privacy and security policies, or an entity may not realize that such information should be carefully safeguarded as well.

For example, health care entities typically have detailed information on past, present, and prospective employees. This information may include Social Security Numbers (SSNs), tax information, fingerprints, signature samples, date of birth, salary and other compensation, bank account numbers for direct deposit, performance evaluations, disciplinary actions or complaints, home address and phone number, and much more. All of this information is, to a greater or lesser extent, considered personal, private, and generally "confidential." Some of the information could be socially or professionally embarrassing to the employee should it be made public. But worst of all, unauthorized disclosure of an employee's confidential information may put that employee at risk for identity theft.

Indeed, the rise of identity theft has made data security an increasing risk area for all employers, including health care entities. In 2005 and 2006, several major health care providers reported breaches of patient and employee information. (Such breaches motivated the Centers for Medicare & Medicaid Services ("CMS") to issue "HIPAA Security Guidance" to provide covered entities with strategies for protecting electronic health information. For an overview of this Guidance see "HIPAA Update" on page 5). Data breaches can occur because of lost or stolen laptops, dumpster diving, dishonest employees, hacking, or for any other number of reasons.

(continued on page 8)

Also In This Issue:

NEW YORK
LONDON
CHICAGO
PARIS
LOS ANGELES
WASHINGTON, D.C.
SAN FRANCISCO
PHILADELPHIA
PITTSBURGH
OAKLAND
MUNICH
ABU DHABI
PRINCETON
N. VIRGINIA
WILMINGTON
BIRMINGHAM
DUBAI
CENTURY CITY
RICHMOND
GREECE

reedsmith.com

Connecticut Attorney General Investigating Possible Anticompetitive Impact of Practice Guidelines

Mr. Blumenthal's investigation should serve as a caution to professional groups contemplating action that could adversely affect competing practitioners or the availability of treatment options.

Medical societies and associations of health professionals routinely adopt and disseminate practice guidelines, opine in position papers, provide expertise, and engage in advocacy before policymakers and, increasingly, before third-party payors on issues of concern to their membership. While these activities are generally designed to promote the highest quality patient care, they often, too, are in the best interest, sometimes the best pecuniary interest, of their members, and sometimes also have the effect of excluding certain products and services from the market.

The recent announcement by Richard Blumenthal, Connecticut's Attorney General, of an investigation into the potentially anticompetitive impact of practice guidelines for the treatment of Lyme Disease—issued this past fall by the Infectious Diseases Society of America ("IDSA" or "Society")—has some in the scientific community crying "foul." At a minimum, however, Mr. Blumenthal's investigation should serve as a caution to professional groups contemplating action that could adversely affect competing practitioners or the availability of treatment options.

Because of the very character of professional associations and learned societies, comprised as they are of individual competitors, and because of the nature of their activities and the reach of their influence, such groups and their members must be highly attentive to the antitrust laws. While some of their actions, such as "lobbying" governmental entities or legislatures on issues of collective concern, are generally immune from antitrust scrutiny, not all the activities of professional associations and learned societies are so protected.

It has long been recognized that by petitioning the government for certain forms of relief, competitors might be able to exclude others from commercial opportunities and thereby cause significant harm to competition. Notwithstanding such potentially anticompetitive results, however, courts have conferred antitrust immunity upon a wide range of activities designed to influence governmental bodies, as long as those activities do not fall within a "sham" exception. This exemption from the antitrust laws for legitimate efforts to influence legislative, administrative or judicial processes is known as the *Noerr-Pennington* doctrine, so named for the two U.S. Supreme Court cases in which the immunity was originally articulated. *See*, *Eastern R.R. Presidents Conference v. Noerr Motor Freight, Inc.*, 365 U.S. 127 (1961); *United Mine Workers v. Pennington*, 381 U.S. 657 (1965). *See also California Motor Transport Co. v. Trucking Unlimited,* 404 U.S. 508 (1972).

However, many actions by professional associations, including those that tend to have the effect of excluding competitors or groups of competitors, *are* subject to antitrust scrutiny. As a general proposition, an association may be liable under Section 1 of the Sherman Act, 15 U.S.C. § 1, for engaging in exclusionary conduct intended to harm providers of products or services that pose a potential competitive threat to its members. Indeed, courts have frequently found professional associations or societies liable for unreasonable exclusionary behavior, including behavior growing out of the adoption of standards,

practice guidelines and the like. *See, e.g., American Society of Mechanical Engineers, Inc. v. Hydrolevel Corp.*, 456 U.S. 556 (1982); *Radiant Burners, Inc. v. Peoples Gas Light & Coke Co.*, 364 U.S. 656 (1961).

Conduct has generally been deemed "exclusionary" not only when the exclusion is literal—such as when an authoritative standard-setting body uses a biased process to declare a product or service to be non-compliant with its standards—but also, for example, when an association of competitors engages in a coordinated campaign of disparagement intended to limit market access by others. In order to evaluate the legality of such conduct by a learned or professional society or association, courts generally apply a "rule of reason," meaning that joint conduct is deemed unlawful only where it is found to have resulted in an "unreasonable restraint on competition." *Continental T.V., Inc. v. GTE Sylvania, Inc.*, 433 U.S. 36, 49 (1977); *see also, FTC v. Indiana Federation of Dentists,* 476 U.S. 447, 458 (1986); *Wilk v. American Medical Ass'n,* 895 F. 2d 352, 359 (7th Cir. 1990).

In order to prevail in a rule of reason analysis, it must first be shown that a defendant possesses power in the relevant market and, then, that the actual or potential negative impact of the challenged conduct on competition in that market outweighs any putative benefits to consumers (or patients). Associations are typically treated as possessing market power if, either directly or through their members, they comprise a substantial portion of competitors in the relevant market or otherwise can be shown to wield substantial influence over competition in that market.

Claims have been brought with some regularity against medical associations and physician groups based also on unreasonable or unfounded disparagement of potentially competitive products or service providers. *See, e.g., Summit Health, Ltd. v. Pinhas*, 500 U.S. 322, 326-27 (1991) (antitrust claim properly stated against ophthalmologists who sought to prevent competition from a practitioner of a lower-cost surgical procedure by disseminating an unfair and biased peer review report); *Wilk v. American Medical Ass'n*, 895 F. 2d 352, 356–57 (7th Cir. 1990) (affirming an antitrust judgment against the AMA based on disparaging and unfounded characterization of chiropractors as "an unscientific cult" and other conduct intended to "eliminate chiropractic" competition), *but see, Schachar v. American Academy of Ophthalmology*, 870 F. 2d 397 (7th Cir. 1989) (rejecting the claim of a group of ophthalmologists performing radial keratotomy surgeries that sued the American Academy of Ophthalmology for labeling the procedure "experimental.").

Lately, more and more third-party payors have been relying on association practice guidelines and "expert" position papers describing treatment options and medical devices as "untested," "unproven," "experimental," and the like to deny coverage for a wide array of treatment options, often with devastating effects on patients. This appears to be the concern driving the Connecticut investigation. Further, Mr. Blumenthal apparently has not ruled out extending his office's inquiry to insurers which deny coverage for chronic Lyme disease,- citing the IDSA guidelines in their coverage statements.

According to a statement by Mr. Blumenthal, the ISDA, through its overly

(continued on page 4)

Would You Like to Receive *HLM* by E-Mail?

If you send your contact information to Leah E. Bradley—by fax, phone, or e-mail—we will send *Health Law Monitor* to you as an Adobe *Acrobat*® file.

Leah E. Bradley · Reed Smith LLP
Phone: 202.414.9335 · Fax: 202.414.9299 · *lbradley@reedsmith.com*

Name

Company

Title

Address

City State Zip/Postal Code

E-mail

"Connecticut Attorney General Investigating Possible Anitcompetitive Impact…" – *continued from page 3*

strict recommendations, might harm Lyme disease patients by effectively limiting their insurance coverage. "These rules diminish the options available to doctors and their patients in ways that can sanction insurance company decisions to deny coverage, so they have an economic impact that could be very serious," Mr. Blumenthal said in an article that appeared in the *Boston Globe* in late December ("Connecticut disputes doctors' Lyme disease guidelines," by Associated Press, Dec. 31, 2006.)

"These rules diminish the options available to doctors and their patients in ways that can sanction insurance company decisions to deny coverage, so they have an economic impact that could be very serious," Mr. Blumenthal said in an article that appeared in the Boston Globe in late December.

The scientific community is alarmed. A recent article in *The Scientist* describes Mr. Blumenthal's investigation as "an unprecedented move that raises questions about the government's role in scientific consensus." ("State official subpoenas infectious disease group," published Feb. 7, 2007). *The Scientist* quotes IDSA's lawyer as saying that, "If we have to worry each time [we craft medical guidelines] that maybe we will be getting subpoenaed and to go through the time, effort, and expense of responding, then we might not take controversial but appropriate positions."

The ISDA, not surprisingly, sticks by the guidelines it enacted in October, which, it contends, were carefully researched and are sound. The Society's website, when last visited April 19, 2007, prominently posted a message from its President, Dr. Henry Masur, in which he described ISDA Practice Guidelines as "valuable, credible, flexible," indeed, "one of the most important activities" of the Society. In his message, Dr. Masur noted that, last year alone, more than 150,000 visitors downloaded the Society's guidelines from the IDSA website. Dr. Masur then went on to describe in some detail how IDSA ensures the quality of its guidelines…an action that he apparently felt compelled to take "(g)iven [the guidelines'] importance, and the recent attention some—particularly the new guidelines on Lyme disease—have received in the media."

At last check, Connecticut's investigation remains open; its outcome uncertain. Mr. Blumenthal's office is in the process of reviewing documents and answers to interrogatories provided by the Society in response to an administrative subpoena issued to the IDSA in November. Whatever the resolution of this particular investigation, the matter should serve to reinforce how carefully associations must tread when their actions might adversely impact competition and, thus, might implicate the antitrust laws.

Judith L. Harris
Washington, D.C.

HIPAA Update

Although it has been 11 years since the passage of the Health Insurance Portability and Accountability Act Of 1996 ("HIPAA") and four years since compliance with HIPAA's first set of administrative simplification requirements was due, those HIPAA requirements continue to impact the day-to-day operations of health care providers, health plans and other health care entities. This article provides a brief update of regulatory, caselaw and enforcement developments on the HIPAA administrative simplification front.

CMS Security Guidance on Portable Devices and Remote Access

The Centers for Medicare & Medicaid Services ("CMS") recently published additional guidance for compliance with the HIPAA Security Rule ("Security Guidance") in order to reinforce some of the ways in which a covered entity may protect electronic protected health information ("EPHI") when it is accessed or used off-site or remotely. Because of the growing number of reported security incidents and increased vulnerability associated with the use of certain portable, remote access, or off-site devices and tools ("off-site devices"), CMS targeted the Security Guidance to a covered entity's use of off-site devices that store, contain, or are used to access EPHI. The Security Guidance lists the following off-site devices as particularly vulnerable to security incidents: laptops; home-based personal computers; PDAs and Smart Phones; hotel, library or other public workstations and Wireless Access Points (WAPs); USB Flash Drives and Memory Cards; floppy disks; CDs; DVDs; backup media; Email; Smart cards; and Remote Access Devices (including security hardware).

Although CMS acknowledged that many situations warrant the off-site use of or access to EPHI, CMS cautioned that such use or access is appropriate only after a covered entity has conducted a risk analysis that (1) examines its business activities to determine the necessity of the off-site use or access; and (2) determines whether its policies, procedures, workforce training, and permitted access to EPHI are consistent with the requirements of HIPAA's privacy and security rules. After a covered entity conducts its risk analysis, the Security Guidance states that the security policies and procedures required by HIPAA should be revised to include appropriate authorization for remote access to EPHI, security requirements for storing EPHI beyond the covered entity's physical control, and transmission processes that ensure the integrity and safety of EPHI that is exchanged both directly and remotely accessed over applications hosted by the covered entity. CMS indicated in the Security Guidance that a covered entity's workforce training should, at a minimum, include clear and concise instructions for accessing, storing, and transmitting EPHI. CMS further indicated that, if applicable, training programs should include password management procedures, prohibitions against leaving devices in unattended cars or public thoroughfares, and prohibitions against transmitting EPHI over open networks or downloading EPHI to public or remote computers.

Security incident procedures must specify the actions workforce members must take in the event that EPHI is lost via portable media; such actions may include securing and preserving evidence, managing the harmful effects of improper use or disclosure of the EPHI, and providing notice to affected parties. In developing sanction policies so that workforce members understand the consequences for non-compliance with policies on remote access to and off-site use of EPHI, CMS urged covered entities to consider requiring employees, as a pre-requisite to employment, to sign a statement of adherence to security policies and procedures.

CMS reminded us in the Security Guidance of its delegated authority to enforce HIPAA's security standards; CMS further stated that it may rely on the Security Guidance to determine whether the actions of a covered entity are reasonable and appropriate for safeguarding the confidentiality, integrity and availability of EPHI, and that the Security Guidance may be given deference in an enforcement hearing.

State Courts Look to HIPAA as Standard

While HIPAA does not provide a private right of action, compliance with HIPAA is being noted by courts in assessing state privacy claims. Two recent examples:

- In a recent Illinois case, compliance with HIPAA standards helped to defeat respondeat superior claims against Illini Hospital. The plaintiff patient in *Bagent v. Blessing Care Corporation*, 244 Ill.2d 154 (2007), asserted that subsequent to her undergoing a blood test at the hospital, a phlebotomist employee revealed in a social setting that the patient was pregnant. The patient's allegations of breach of patient confidentiality, invasion of privacy and infliction of emotional distress were made against the phlebotomist, and also against the hospital on the theory of respondeat supe-

(continued on page 6)

"HIPAA Update" – *continued from page 5*

rior. In a reversal of the appellate court's denial of the hospital's motion for summary judgment, the Illinois Supreme Court reviewed evidence that the hospital provided HIPAA privacy training to its employees, including the phlebotomist, and that the phlebotomist understood from the training that patient information should not be disclosed. The court's conclusion that the phlebotomist's disclosure of the patient's information was not the kind of conduct she was hired to perform was, in large part, based on the evidence that Illini Hospital had provided HIPAA training to its employees.

- In *Acosta v. Byrum*, 638 S.E.2d 246 (N.C. Ct. App. 2006), a psychiatric patient brought claims of invasion of privacy and infliction of emotional distress against a psychiatrist and office manager who allegedly improperly accessed and disseminated the patient's health information. The plaintiff alleged that the psychiatrist improperly permitted the office manager to use the psychiatrist's medical records access code in violation of hospital rules and regulations, and in violation of HIPAA. The trial court had dismissed the case, in part on the grounds that HIPAA does not provide a private right of action. In reversing the trial court's dismissal of the claims against the psychiatrist, the North Carolina Court of Appeals found that the plaintiff had not made a HIPAA claim, but found instead that HIPAA provided a standard of care in determining whether the physician defendant properly maintained the privacy of a patient's confidential medical records.

Both the* Bagent *and* Acosta *cases demonstrate that HIPAA compliance is not simply a federal regulatory matter.

Both the *Bagent* and *Acosta* cases demonstrate that HIPAA compliance is not simply a federal regulatory matter. In assessing state privacy claims, courts are now looking to HIPAA as a standard of care for protecting the privacy of health information.

NPI Deadline Almost Here

After May 23, 2007, HIPAA requires covered entities—most health plans, health care clearinghouses and most health care providers—to use the National Provider Identifier ("NPI") on all standard transactions where a health care provider's identifier is required. The NPI rule requires health care providers to obtain an NPI from the National Provider System; health care providers may apply for the NPI through a web-based application process at *https://nppes.cms.hhs.gov*.

In Guidance issued April 2, 2007 ("NPI Guidance"), CMS announced that it will allow covered entities that are unable to fully comply with the NPI requirements by the compliance date to implement contingency plans in order to allow additional time to carry out testing and other activities without payment disruption. CMS stated in the NPI Guidance that for 12 months after the compliance date, CMS will not impose penalties if covered entities have deployed contingency plans and have made reasonable and diligent efforts to become compliant. In a recent response to a frequently asked question ("FAQ") on its website, CMS urged providers that have not yet obtained NPIs to do so immediately, and stated that failure to obtain an NPI may be viewed as a violation of the good faith provisions of the NPI Guidance. Other FAQs and CMS responses regarding implementation of the NPI can be found at

http://www.hhs.gov/faq/medicaremedicaid/2009.html.

First HIPAA Conviction at Trial

In the first HIPAA violation case to go to trial, a Fort Lauderdale jury convicted Fernando Ferrer, Jr. on Jan. 24, 2007 of computer fraud, conspiracy to defraud the United States, aggravated identity theft, and the wrongful disclosure of protected health information under HIPAA. The case involved the theft and transfer of Medicare patient information from the Cleveland Clinic in Weston, Fla. Ferrer purchased the patient information from a former Cleveland Clinic employee, who pleaded guilty to similar charges and testified against Ferrer. The theft resulted in the submission of more than $7 million in fraudulent Medicare claims. In addition to a maximum sentence of 20 years for the non-HIPAA counts, Ferrer faces up to 10 additional years in prison for wrongfully disclosing protected health information.

Enforcement Notes

According to the Department of Health and Human Services, as of Dec. 31, 2006, the Office for Civil Rights ("OCR") received a total of 24,000 HIPAA privacy complaints. Of those complaints, more than half were not investigated because (1) the complaints were untimely filed, (2) OCR did not have jurisdiction over the covered entity named in the complaints, or (3) the allegations did not constitute violations of the Privacy Rule. OCR has investigated and closed approximately 6,000 complaints, and took informal enforcement action in 4,025 of those cases. As of the end of 2006, OCR had referred more than 300 cases to the Department of Justice.

Katherine M. Keefe
Brad M. Rostolsky
Philadelphia

Recent Reed Smith Client Memoranda Available

Date	Title
4/16/07	New York Enacts State False Claims Act and Steps Up Medicaid Fraud Enforcement
3/5/07	FDA Issues Public Health Notification About Potential Risks Associated With Change in Date for Daylight Savings Time
2/9/07	Recent Changes to Executive Order 12866 Increases OMB Oversight of Agency Guidance Documents and Regulatory Activities
1/8/07	Tax Relief and Health Care Act of 2006 Signed into Law with Major Medicare & Medicaid Provisions
11/17/06	FDA Guidance on Prescription Drug Marketing Act
10/31/06	California Update: New Laws on Adverse Event Reporting and Facility Inspection
10/25/06	HHS OIG Work Plan for Fiscal Year 2007
10/3/06	Final Anti-Kickback Safe Harbors and Stark Exceptions for Electronic Prescribing and Health Records Arrangements
6/16/06	Supreme Court "Third-Party Payor" Decision: *Arkansas Department of Health and Human Services v. Ahlborn*

If you would like copies of any of the above-listed memoranda, please contact a member of our Health Care Group, who will be happy to send them to you.

"How to Prevent (or Respond to) a Data Security Breach and Identity Theft" – *continued from page 1*

A carefully-considered mix of administrative, physical, and technical safeguards (on top of existing HIPAA policies for those covered entities that are subject to HIPAA) will serve to minimize the likely incidence and impact of a breach.

There is no silver bullet solution to guarantee that a health care entity will not have to confront a data security incident. However, a carefully considered mix of administrative, physical, and technical safeguards (on top of existing HIPAA policies for those covered entities that are subject to HIPAA) will serve to minimize the likely incidence and impact of a breach.

So, what can health care entities do to prevent a data security breach?

- ***Take Stock.*** Get an understanding of the quantity and nature of confidential information your entity gathers, stores, uses, shares, destroys. It is easy for the flow of confidential information to take on a life of its own as technology—and the processes, policies, and procedures of an entity—evolves over the years. Knowing what confidential information your entity has and how it travels within the entity is the first step in protecting it.

- ***Develop a Realistic Policy for Safeguarding Data and Stick With It.*** Ideally, a data security policy will incorporate input from all employees who will be protecting the information on a day-to-day basis. What may sound like a good idea to a policy planning committee (*e.g.*, encrypting all computers or requiring vendors to adopt certain information-safeguarding policies) may not be technically feasible or cost-effective, or may run at cross-purposes with existing policies. It is better to have a modest, practical plan that is actually executed, than a comprehensive plan that sits on a shelf.

- ***Make Your Security Policy Multidimensional.*** Many security breaches happen because health care entities consider data security to be an IT issue. The best IT department in the world won't stop a breach involving paper records, burglars, or disgruntled employees. Safeguarding data requires an administrative element—particularly ongoing management buy-in that is effectively communicated to employees. Safeguarding also requires a physical security element that involves thinking about how confidential information is stored, accessed, transmitted, and protected against intrusion, especially at off-site locations. And, yes, safeguarding requires an ongoing technical review of how technology is set up and used.

- ***Keep Abreast of Best Practices.*** As of this publication, there is no federal statutory standard for protecting non-medical, non-financial personal data. The applicable standard is negligence, *i.e.*, confidential information must be reasonably protected. Thus far, best practices are industry-specific and industry-developed. In the health care industry, the HIPAA Security Rule provides a good roadmap for best practices, even for non-HIPAA protected information. *See* 45 C.F.R. Parts 160 and 164 Subpart A and C. In particular, as previously mentioned, the recent "HIPAA Security Guidance" issued by CMS outlines a number of best practices for protecting electronic health information, such as implementing two-factor authentication for granting remote access to systems that contain health information.

- ***Publicize It and Train on It.*** Protecting confidential information is the business of all employees, agents, contractors or volunteers who have access to confidential information that was entrusted to your health care entity. Widespread awareness of the importance of protecting all confidential information is the best defense an entity can have against a serious breach.

If, despite its best efforts, a health care entity experiences a security breach, what should it do?

- ***Have a Good Security Breach Response Policy and Follow It.*** The policy should state the entity's intent to fully and completely respond to any report of a security breach, and its commitment to minimize the impact of any breach. The policy should require reporting any suspected security breach to one clearly identified management-level employee (*e.g.*, a Privacy Officer). It should also incorporate the elements outlined below.

- ***Assemble a Working Group.*** Once the Officer is notified of the breach (or potential breach), he or she should then assemble and lead a working group to investigate and respond to the breach, as appropriate. The group may be comprised of as many people as appropriate, usually a representative from the legal department and a person with responsibility in the affected department (*e.g.*, Human Resources).

- ***Investigate the Breach.*** The working group must thoroughly investigate the breach, including interviewing anyone with knowledge of the incident and conducting an examination of the physical and technical security.

- ***Determine Whether to Notify any Affected Individuals.*** To the extent the security breach involves personal information, the entity should assess whether the individuals who are the subject of such information should be notified. This involves an assessment of both federal and state law. At this time, only 35 states have mandatory security breach notification laws. There are no federal requirements. The entity should also determine whether any policy, contract or best practice dictates notification of the affected individual(s). For example, where an individual's Social Security Number, name and address is stolen, that individual may be at risk for identity theft, which may make notification prudent.

- ***Consider Providing Affected Individual(s) With Assistance.*** For example, the entity may want to provide the individual with information on how to contact credit bureaus and freeze new lines of credit. The entity may also consider offering to pay for credit monitoring services.

- ***Determine Whether to Notify Law Enforcement or Other Agencies.*** If the working group investigating the breach has reason to believe that the reported event involved a criminal act (*e.g.*, credit card fraud), it should notify and cooperate with appropriate law enforcement authorities (*e.g.*, local police). The working group must also determine whether any duty exists to notify state officials and/or consumer reporting agencies, and, if so, must make such notification.

- ***Assess and Implement Other Mitigation Measures.*** The working group should consider, and implement, as appropriate, other methods to mitigate the impact of any security breach. This may involve enhancements to physical or technological security, additional employee training on specific privacy or data security procedures, and/or increased supervision over access to confidential information. Finally, individuals who violate a security breach policy should be disciplined, as appropriate.

In sum, it is critical that every health care entity have comprehensive privacy and security policies in place—including those for responding to a data security breach. In the event of a breach, an entity should immediately assess the specific factual circumstances surrounding the breach, remedy the breach at issue and the look for ways to systematically improve the way it protects confidential information in its possession.

Paul Bond
Princeton

Gina M. Cavalier
Washington, D.C.

Pulse

Health Care

Reed Smith's Health Care Group was named one of "America's Top Health Litigators" by *HealthLaw360*.

Scot T. Hasselman was named one of the "Outstanding Young Healthcare Lawyers" in the United States by *Nightingale's Healthcare News*. In addition, Scot presented regarding "Medicare and Medicaid" at an ABA Teleconference on Medicaid/Medicare in September.

Elizabeth Carder-Thompson was profiled as an "Outstanding Woman Attorney" by *HealthLaw360*.

Julia Krebs-Markrich was named one of the "Outstanding Hospital Lawyers" in the United States by *Nightingale's Healthcare News*.

Thomas C. Fox was named one of the "Outstanding Fraud and Compliance Lawyers" in the United States by *Nightingale's Healthcare News*.

Daniel A. Cody was elected a Council Member of the American Bar Association's Health Law Section (term expiring in 2009). He also wrote "A Medicare Benefits Primer," which appeared in *The Practical Lawyer* in October.

James M. Wood became Chairman of the Board for the Food and Drug Law Institute ("FDLI") Nov. 19 for a one-year term. Jim also received the "Lawyer of the Year" award from San Francisco's AIDS Legal Referral Panel. In addition, Jim wrote an article entitled, "Courts Give Mixed Reviews to Preemption Policy in 2006 FDA Labeling Rule," which appeared in the Washington Legal Foundation's "Critical Legal Issues, Working Papers Series" in January. Jim and **Areta L. Kupchyk** spoke in September at CBI's Annual Product Recalls Summit held at the Marriott Indianapolis Downtown in Indianapolis. Areta and Jim presented a program entitled, "Essential Requirements During a Class I Recall—The Fundamentals."

In October, **Areta L. Kupchyk** participated in the PLI Conference "Pharmaceutical Law 2006: Across the Product Life Cycle," held in New York. Areta presented regarding "R&D 101: Overview of the Legal Issues During Research Development." Additionally, Areta and **George Pickering** wrote an article entitled "Route to Market for Tissue and Cell-Based Therapeutics: The US and Europe," which was published by the Practice Law Company ("PLC") in a *Cross-Border LifeSciences Handbook*.

Lorin E. Patterson was named to *Today's SurgiCenter's* fourth annual "Who's Who in the Ambulatory Surgery Industry" list. In addition, Lorin and **Cynthia A. Alcantara** spoke at the Third Annual Surgicenter Conference at Mandalay Bay Resort and Casino in Las Vegas. They presented regarding topics which included "Regulatory, Legal and Legislative Update," "Legal Strategies for Recruiting and Removing Physician Members," and "Top 10 Tips for Profitability of ASCs."

Gail L. Daubert spoke in October regarding "The Challenges and Opportunities in the Use of Off Label Drugs

and Devices," at a Society for Women's Health Research meeting.

Thomas W. Greeson spoke in September at the Imaging Center Symposium in Las Vegas. Also in September, he spoke at the American Roentgen Ray Society ("ARRS") Educational Program: "Cardiac CT Angiography, A Practical Approach," in Chicago. Tom presented regarding "Legal Issues with Cardiac CT Angiography Interpretation Agreements." In addition, Tom spoke at the Radiology Business Managers Association Fall Conference, at the Educational Symposia's 21st Annual Economics of Diagnostic Imaging 2006 National Symposium held in Arlington, and at the American Roentgen Ray Society meeting held in San Diego in early February. Tom wrote numerous articles, including: "Hasty Budget Action Spurs Petition for Delay," which appeared in September's edition of *Diagnostic Imaging*; "Utilization Management Firms Grow Big Business To Little Practical Effect," which was published in the October issue of *Diagnostic Imaging*; "Be Mindful of Stark in CCTA Alliance," which was featured on ImagingBiz.com; "Fall Means Open Season On Imaging Payments: Annual Release of Medicare Update Reveals Multiple Proposals Affecting Radiologists," which was published in the November edition of *Diagnostic Imaging*; "Legally Speaking - Physician Extenders in the IR Practice Billing for Services," which appeared in *IR News*; and "Beware of Precertifying Procedures for Referrers," which was in December's issue of *Diagnostic Imaging*.

Carol Colborn Loepere and **Katherine M. Keefe** spoke in September at the PHCA/CALM (Pennsylvania Health Care Association/Center for Assisted Living Management) Annual Convention held in Seven Springs Mountain Resort, regarding Medicare Part D. Carol also spoke in February at the American Health Lawyers' Association "Long Term Care and the Law" Conference, which was held in Orlando. Her presentation was entitled, "Introduction to Long Term Care."

At IBC Life Science's "5th Annual Molecular Diagnostics/Discovery 2 Diagnostics Conference" held in September at the Hynes Convention Center in Boston, **Gordon B. Schatz** spoke regarding "Reimbursement Issues."

In October, **Robert J. Hill** and **Joseph W. Metro** participated in ACI's "6th National Forum on Fraud & Abuse in the Sales and Marketing of Drugs," held in New York. In addition, Bob spoke at Pharmaceutical Education Associates' "Prescription Drug Pricing 101 and 102 Conference," which was held in February in Philadelphia.

Joseph W. Metro and **Robert J. Kaufman** attended ACI's "5th National Conference on Avoiding Regulatory Scrutiny in the Sales and Marketing of Medical Devices," held in November at The Sutton Place Hotel in Chicago. Joe gave a presentation at the conference regarding "Fraud and Abuse."

Karl A. Thallner, Jr. and **Brad M. Rostolsky** wrote an article entitled, "Stark and Reassignment Rule Changes Proposed," which appeared in January in *Physician's News Digest*.

At ACI's Government Investigation Preparedness for Pharma Conference, held in January in New York, **Eric A. Dubelier** spoke regarding "Developing the Playbook for New Domestic and International Challenges."

Kevin R. Barry presented a program at ABA's Health Law Section meeting in February regarding "Stark Law Basics."

Alison J. Dennis wrote an article entitled, "Due Diligence in the European Medical Devices Industry," which was published in December in the *PLC Cross-border Life Sciences Handbook*. Alison also authored "Paediatric Indications and the New Regime for Marketing Authorisations in Europe," a client bulletin which was sent to clients in February.

REED SMITH HEALTH CARE GROUP

Lisa S. Albright	lalbright@reedsmith.com	609 524 2031
Cynthia A. Alcantara	calcantara@reedsmith.com	703 641 4306
Kevin R. Barry	kbarry@reedsmith.com	202 414 9488
Christine E. Bloomquist	cbloomquist@reesmith.com	202 414 9212
Elizabeth Carder-Thompson	ecarder@reedsmith.com	202 414 9213
Gina M. Cavalier	gcavalier@reedsmith.com	202 414 9288
Daniel A. Cody	dcody@reedsmith.com	415 659 5909
J. Ferd Convery, III	jconvery@reedsmith.com	609 514 5940
Gail L. Daubert	gdaubert@reedsmith.com	202 414 9241
David E. Dopf	ddopf@reedsmith.com	609 524 2030
Catherine A. Durkin	cdurkin@reedsmith.com	202 414 9229
Thomas C. Fox	tfox@reedsmith.com	202 414 9222
Thomas W. Greeson	tgreeson@reedsmith.com	703 641 4242
Scot T. Hasselman	shasselman@reedsmith.com	202 414 9268
Jason M. Healy	jhealy@reedsmith.com	202 414 9245
Robert J. Hill	rhill@reedsmith.com	202 414 9402
Robert J. Kaufman	rkaufman@reedsmith.com	202 414 9407
Katherine M. Keefe	kkeefe@reedsmith.com	215 851 8863
Henry R. King	hking@reedsmith.com	609 514 5941
Murray J. Klein	mklein@reedsmith.com	609 520 6022
Julia Krebs-Markrich	jkrebs-markrich@reedsmith.com	703 641 4232
Areta L. Kupchyk	akupchyk@reedsmith.com	202 414 9362
Carol C. Loepere	cloepere@reedsmith.com	202 414 9216
Kevin M. Madagan	kmadagan@reedsmith.com	202 414 9236
Debra A. McCurdy	dmccurdy@reedsmith.com	703 641 4283
Frances Meehan	fmeehan@reedsmith.com	312 207 6468
Joseph W. Metro	jmetro@reedsmith.com	202 414 9284
Robert K. Neiman	rneiman@reedsmith.com	312 207 6546
Karen L. Palestini	kpalestini@reedsmith.com	609 520 6037
Lorin E. Patterson	lpatterson@reedsmith.com	703 641 4368
Paul W. Pitts	ppitts@reedsmith.com	415 659 5971
Steven B. Roosa	sroosa@reedsmith.com	609 514 5983
Brad M. Rostolsky	brostolsky@reedsmith.com	215 851 8195
Gordon B. Schatz	gschatz@reedsmith.com	202 414 9259
Wendy H. Schwartz	wschwartz@reedsmith.com	212 549 0272
Tamara V. Scoville	tscoville@reedsmith.com	202 414 9239
Nancy A. Sheliga	nsheliga@reedsmith.com	804 344 3439
Keith T. Shiner	kshiner@reedsmith.com	703 641 4221
Michael A. Smith	masmith@reedsmith.com	215 851 8179
Abraham J. Stern	ajtern@reedsmith.com	312 207 6465
Thomas H. Suddath, Jr.	tsuddath@reedsmith.com	215 851 8209
Karl A. Thallner, Jr.	kthallner@reedsmith.com	215 851 8171
Eugene Tillman	etillman@reedsmith.com	202 414 9244
Kathryn R. Watson	kwatson@reedsmith.com	415 659 5905
Heather M. Zimmerman	hzimmerman@reedsmith.com	703 641 4352

CONTRIBUTORS TO THIS ISSUE

Paul Bond
Princeton
609 520 6393
pbond@reedsmith.com

Gina M. Cavalier
Washington, D.C.
202 414 9288
gcavalier@reedsmith.com

Judith L. Harris
Washington, D.C.
202 414 9276
jlharris@reedsmith.com

Katherine M. Keefe
Philadelphia
215 851 8863
kkeefe@reedsmith.com

Brad M. Rostolsky
Philadelphia
215 851 8195
brostolsky@reedsmith.com

Health Law Monitor is published by Reed Smith to keep clients and friends informed of developments in health law. It is not intended to provide legal advice to be used in a specific fact situation; the contents are for informational purposes only.