Final breach notification rules pursuant to the American Recovery and Reinvestment Act of 2009 (ARRA) have been released by the Federal Trade Commission (FTC) (the "FTC Breach Notification Rule") and the U.S. Department of Health and Human Services (HHS) (the "HIPAA Breach Notification Rule"). The HIPAA Breach Notification Rule applies to entities and business associates covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), while the FTC’s Breach Notification Rule applies to vendors of personal health records (PHR) and related entities. In some cases an entity may be subject to both rules.

The HIPAA Breach Notification Rule

The Health Information Technology for Economic and Clinical Health (HITECH Act) provisions contained within ARRA require HIPAA-covered entities and business associates to address and incorporate breach notification as an integral part of their HIPAA systems, policies, procedures and training. The HIPAA Breach Notification Rule is anticipated to become effective for breaches occurring on or after September 23, 2009. However, as described below, enforcement will be delayed.

The HIPAA Breach Notification Rule largely follows the HITECH Act, Section 13402, with several important clarifications and modifications. It also provides additional guidance on the technologies and methodologies that render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals, and therefore not considered "unsecured PHI" subject to the breach notification provisions.

Notice of Breach of PHI

A covered entity, following the discovery of a "breach of unsecured protected health information" is required to notify each individual whose PHI has been, or is reasonably believed to have been "accessed, acquired, used, or disclosed as a result of such breach." The notice must be provided without unreasonable delay and in no case later than 60 days after discovery of a breach. For breaches involving 500 individuals or more, the covered entity also must notify HHS concurrently. For breaches involving less than 500 individuals, the covered entity need only maintain a log and report such breaches to HHS annually. Media notice publication or broadcast is also required when a breach involves the PHI of more than 500 individuals. Additionally, covered entities and their business associates must publish substitute notice (e.g., a notice conspicuously posted on the covered entity’s website, or a newspaper or broadcast media notice) where insufficient or out-of-date contact information exists to notify affected persons.

Notifications must include, among other things, a description of the types of PHI subject to the breach. However, the notification also must avoid further disclosure of PHI, such as social security numbers, diagnosis information or account numbers.
The notice to individuals must be written in plain language and comply with applicable federal laws governing appropriate accommodations for persons with limited English language proficiency or sensory disabilities.

Timing of Notice

The HIPAA Breach Notification Rule clarifies that a covered entity’s breach notification “clock” begins ticking as soon as a business associate for the covered entity discovers the breach, making contractual notice and cooperation requirements imperative in business associate agreements. Furthermore, the requirement that no “unreasonable delay” occur prior to notification highlights the importance of appropriately training workforce and other agents to notify the Privacy Official immediately when a potential breach occurs. HHS views the 60-day notification deadline as an outside limit. However, covered entities are expected to take a reasonable time to collect the information required for the notice. Therefore, in some cases multiple mailings may be needed as information becomes available.

Determination Process

A covered entity must undertake a three-step process for determining when a breach notification must be made:

- Was there a data breach? For example, was there an unauthorized acquisition, access, use or disclosure of PHI that was not secured by one of the methodologies approved by HHS for rendering the PHI unusable, unreadable or indecipherable?

- Did the access, acquisition, use or disclosure violate HIPAA privacy and security standards?

- Did the unauthorized access, acquisition, use or disclosure compromise the security or privacy of the PHI, by posing a significant risk of financial, reputational, or other harm to the individual?

The third step, above, creates a so-called harm threshold and necessitates that covered entities determine and document the risk of harm to the individual resulting from a potential breach of unsecured PHI.

The rule further clarifies that the security or privacy of the PHI is not compromised unless there is a "significant risk of financial, reputation, or other harm to the individual." In some cases the PHI may be recovered so quickly (such as the recovery of a lost laptop computer where forensic analysis shows that no acquisition or disclosure of PHI occurred) or so limited in content, that the risk of harm is so low that a notification of breach may be avoided. Caution is advised when conducting such analyses, however, as the HIPAA Breach Notification Rule places the burden of demonstrating compliance squarely on the shoulders of the covered entity. It also provides that the security or privacy of the information is not considered compromised, if only certain narrowly-defined elements are affected. HHS cautions, however, that this is a very narrow exception and must not be construed as permitting or encouraging the use or disclosure of more than the "minimum necessary" PHI in violation of the limits and requirements found in 45 C.F.R. Sections 164.502(b) and 164.514(d).

Encryption Issues

Finally, the HIPAA Breach Notification Rule clarifies that the methodologies approved to render PHI unusable, namely encryption and destruction, relate only to the HIPAA Breach Notification Rule and are viewed separately and apart from the HIPAA security standards. Consequently, an encryption method that complies with HIPAA security standards will not necessarily comply with the HIPAA Breach Notification Rule. With respect to encryption, HHS advises that the confidential process or key to decrypt data must be stored on a device or housed in a location separate from the data they encrypt or decrypt.
HHS also clarifies that redaction is not an approved method of destruction.

**Enforcement Delay**

Perhaps the most immediately significant development contained in the HIPAA Breach Notification Rule is the decision by HHS to delay enforcement and the imposition of sanctions during the 180-day period following publication. Despite some initial "breathing room" on the enforcement side, HHS expects that covered entities and business associates will be in compliance with the HIPAA Breach Notification Rule on the effective date (September 23, 2009).

See the display copy of the interim final rule.

**The FTC Breach Notification Rule**

Originally proposed in April 2009, the FTC Breach Notification Rule requires compliance by vendors of PHR, such as web-based repositories used for tracking an individual’s health information and entities offering third-party applications for PHRs, such as information uploaded from a blood pressure cuff or pedometer. The final FTC Breach Notification Rule clarifies that it applies both to vendors of PHR and related entities, irrespective of any jurisdictional tests. Consequently, a wide variety of entities are subject to its requirements.

**Application of the Rule**

The FTC Breach Notification Rule does not apply to HIPAA-covered entities or business associates, including for example, instances involving physicians who offer a PHR to their patients. To avoid consumers receiving duplicate notices for the same breach, the FTC clarifies that if a PHR vendor is both a business associate and deals directly with consumers, it need not notify a customer receiving a breach notification on behalf of a HIPAA-covered entity (discussed above).

In response to comments expressing concern that third-party vendors would not be aware that they were handling covered electronic health records, the FTC added a provision to the Breach Notification Rule that requires vendors of PHR and PHR-related entities to notify third-party service providers of such status.

The requirements under the federal breach notification law supersede any contrary provision of state law, in the same manner as the HIPAA privacy rules supersede state law. The FTC Breach Notification Rule, however, does not preempt state laws imposing additional, as opposed to contradictory, breach notification requirements.

Additionally, the FTC Breach Notification Rule eliminated many of the barriers from the proposed rule to sending e-mail notification to consumers. However, consumers must be given a clear, conspicuous and reasonable opportunity to receive breach notifications by first-class mail. The time period a breach is required to be posted on an entity’s website also was reduced from six months to 90 days. The FTC has developed a form for vendors of PHRs or PHR-related entities to use in notifying the FTC of a breach. The information received by the FTC will be entered into a searchable database that will be made available to the public.

**Timing of Notice**

Finally, the FTC Breach Notification Rule clarifies that the 60-day period for the breach notification may begin before an entity establishes that all of the prerequisites for triggering a breach notification have been determined. The FTC stated that the 60-day period is to give entities time to conduct such an investigation. Hence, the clock starts ticking very early on and will not be delayed until the "entity conducts an investigation to determine whether unauthorized acquisition has occurred, whether PHR identifiable health information has been breached, or whether the information breached was unsecured."

See a display copy of the final rule.

For more information, please contact John S. Mulhollan, jmulhollan@bakerlaw.com or 216.861.7484, or Steven A. Eisenberg, seisenberg@bakerlaw.com or 216.861.7903.

---

THE JOINT COMMISSION AND AMA TACKLE DISRUPTIVE BEHAVIOR BY PHYSICIANS
In the past year, both The Joint Commission (TJC) and the American Medical Association (AMA) have addressed the issue of “disruptive behavior” by physicians, though they do not necessarily agree on what that term means or what should be done in response to such behavior.

**The Joint Commission Issues Revised Standards**

In 2008, TJC revised two of its Standards for Hospital Accreditation, LD 03.01.01 and MS 4.00. LD 03.01.01 now requires all hospitals to have a code of conduct that “defines acceptable, disruptive and inappropriate behaviors.” In addition, “interpersonal skills” and “professionalism” have been added to the MS 4.00 list of core competencies to be reviewed by a hospital in making credentialing and privileging decisions. While neither Standard defines “disruptive” or “inappropriate” behavior, TJC explained in its July 9, 2008, Sentinel Event Alert, that such term has a very broad meaning. “Disruptive” or “inappropriate” behaviors, according to TJC, include both overt, egregious actions, such as “verbal outbursts and physical threats,” as well as passive actions or inactions, such as “refusing to perform assigned tasks,” “quietly exhibiting uncooperative attitudes during routine activities,” “reluctance or refusal to answer questions, return phone calls or pages,” “condescending language or voice intonation” and “impatience with questions.” TJC goes on to advocate education of all staff on appropriate professional behavior, a task that may be very difficult when the medical staff is comprised of independent physicians, and a zero-tolerance policy for particularly bad actions such as assault and other criminal acts. While the Alert does promote “non-confrontational interventional strategies . . . progressing to disciplinary proceedings if behavior does not cease,” it does not specifically address due process in disciplinary procedures.

**The AMA Weighs In**

TJC’s broad definition of “disruptive” and “inappropriate” behavior, along with its silence on the issue of due process, led the AMA to draft its own Model Staff Code of Conduct. The AMA separates “inappropriate behavior,” defined as “conduct that is unwarranted and is reasonably interpreted to be demeaning or offensive” and warranting a much lighter disciplinary approach, from “disruptive behavior,” defined as “abusive conduct involving sexual or other forms of harassment, or other forms of verbal or non-verbal conduct that harms or intimidates others to the extent that quality of care or patient safety could be compromised” and warranting a more serious disciplinary approach. While persistent “inappropriate behavior” may rise to the level of “disruptive behavior,” the AMA also has explicitly exempted other types of behavior from discipline altogether. These include good faith criticisms, actions encouraging clear communication, expressions of concern about a patient’s care and safety, expressions of dissatisfaction with hospital policy if communicated through appropriate complaint procedures and the use of a cooperative approach to problem-solving. Like TJC, the AMA also advocates initial, non-confrontational approaches to resolve inappropriate behaviors. Unlike TJC, however, the AMA also strongly emphasizes the importance of not denying the accused physician due process throughout the disciplinary process.

**Impact on Hospitals**

Regardless of the approach adopted, the following conclusions are evident: hospitals must adopt a code of conduct and medical staff bylaws that address disruptive or inappropriate actions by physicians and other staff, and the hospital must preserve due process in disciplining such individuals. While TJC’s definition of “inappropriate behavior” may be viewed by some to encompass a whole host of innocuous actions, hospitals must realize that not all aggressive actions, complaints or other such behaviors are subject to discipline. The hospital also must look to the statutory and case law in its state for guidance. Additionally, TJC’s recommendations do not affect in any way the due-process safe harbor under the Health Care Quality Improvement Act. If medical staffs want to continue to enjoy immunity from money damages for their peer review conduct, they will continue to follow the due process procedures set forth in their bylaws, including providing the accused physician with adequate notice of and procedures for any hearing and conducting such hearings with fundamental fairness.

For more information, please contact Emily E. Williams, eewilliams@bakerlaw.com or 216.861.7373.

---

**OIG Concerned About Incident to Services Rendered by Unqualified Personnel**

Medicare Part B covers certain services that are billed by physicians but are performed by nonphysician practitioners “incident to” the services of a physician. According to the HHS Office of Inspector General (OIG), “incident to” services are vulnerable to overutilization and may put beneficiaries at risk of receiving services that do not meet professionally recognized standards of care.

**The OIG Study**

---
A recent study by the OIG of “incident to” services performed by nonphysician personnel found that “unqualified” nonphysician personnel performed 21 percent of the services that physicians did not perform personally. Nonphysician personnel in the study sample included technicians, nurses, licensed or certified assistants, therapists and other employees who were not licensed or certified but instead had received other formal medical training, on-the-job training, or no formal medical training whatsoever. According to the OIG, these nonphysician personnel lacked the necessary licenses or certifications, had no verifiable credentials or lacked the training to perform the service at issue. The OIG also found that unqualified personnel performed seven percent of invasive services that physicians did not perform.

Recommendations for CMS

As a result of the study, the OIG recommended that the Centers for Medicare and Medicaid Services (CMS):

- Seek revisions to the “incident to” rule, to require that physicians who personally do not perform services they bill to Medicare ensure that such services are performed by other licensed physicians or are performed under the direct supervision of a licensed physician by nonphysicians who have the necessary training, certification and/or licensure to perform the services;

- Require physicians who bill services to Medicare that they do not personally perform to identify the services on their Medicare claims by using a service code modifier, which would allow CMS to monitor claims to ensure that physicians are billing for services performed by nonphysicians with appropriate qualifications; and

- Take action to address the claims that were detected that were billed by physicians and performed by nonphysicians that were not “incident to” services and were for rehabilitation therapy services performed by nonphysicians who did not have the training of a therapist.

CMS agreed with the OIG’s first recommendation, noting that it was in the process of clarifying manual policies addressing “incident to” billing, including guidance for documenting the qualifications of a person performing services “incident to” the services of a physician. As to the second recommendation, CMS agreed in principle but contended it would be difficult to implement operationally. As a result, CMS has promised to study the issues involved in adding code modifiers to services furnished exclusively by staff other than the billing physician. CMS also concurred with the third recommendation and agreed to share the OIG report with the Medicare Administrative Contractors (MACs).

Intensified Scrutiny by CMS

It appears that CMS’s scrutiny of “incident to” services will intensify; therefore, all providers should begin to take actions to verify and ensure that nonphysician personnel who are rendering services incident to those of a physician have the appropriate qualifications to do so. See the OIG report.

For more information, please contact Krista M. Barnes, kbarnes@bakerlaw.com or 713.646.1352.

PURCHASING COSTS UNDER THE MICROSCOPE

An August 11, 2009, letter sent jointly by Sens. Charles Grassley (R-Iowa), Herb Kohl (D-Wis.) and Bill Nelson (D-Fla.) on behalf of the Senate Judiciary Committee’s Antitrust, Competition Policy and Consumer Rights Subcommittee to MedAssets, Novation, Amerinet, Broadlane, Consorta, Premier and the HealthTrust Purchasing Group (collectively, GPOs), suggests that the Subcommittee is beginning to scrutinize some of the healthcare industry’s structural costs as part of healthcare reform in an effort to increase the transparency of the provider purchasing process.

Limited Information Available

The senators were concerned that there was limited information about the services and activities performed by GPOs and how the GPOs were paid for their services. The senators stated “there is little information about other fees or payments that GPOs may secure from manufacturers, other vendors and suppliers, in connection with and outside of group purchasing activities, such as product marketing.” GPOs historically have argued that they would not be able to offer programs beyond basic contracting services without the fees, which traditionally have been paid by product manufacturers. The argument, however, appears to have intrigued the senators, as they have asked the GPOs to document and explain their non-contracting services and to see detailed information on how the GPOs interacted with providers, manufacturers, vendors and suppliers, including data regarding the fees charged and the impact on the GPO and its members when a member hospital purchases items outside of the GPO agreement.
False Claims Action

At least one whistleblower lawsuit under the federal False Claims Act bears watching. *United States ex rel. Fitzgerald v. Novation LLC*, S.D. Tex., No. 3:03-CV-01589. In this case, a former Novation employee alleged that from 1993 to 2003, Novation and others used their market power to secure kickbacks and other illegal remuneration from vendors in exchange for awarding them GPO contracts. The whistleblower claimed that the fees were well hidden through "slush funds," secret accounts and unrelated business ventures. In addition, the whistleblower alleged that her compensation rewarded her for closing deals that maximized the payments to the GPO rather than finding the lowest bid for the GPO’s members.

Physician Payments Sunshine Act

The GPO inquiries follow the reintroduction of the Physician Payments Sunshine Act (PPSA) earlier this year by Sens. Grassley and Kohl. The PPSA requires GPOs to disclose all payments or transfers of value to physicians worth $100 or more. The PPSA would require payments and other transfers of value for consulting fees, compensation for other services, honoraria, gifts, entertainment, food, travel, education, research, charitable contributions, royalty or license fees, current or prospective ownership or investment interests, CME speaker fees and grants and other payments to be reported to CMS in a searchable manner. Manufacturers or group purchasing organizations that fail to report such payments would be subject to fines between $1,000 and $10,000 per infraction, up to a total fine of $150,000 per company per year, where the failure to report is deemed to be an oversight. However, if the failure is a "knowing failure to report," the aggregate annual fine limit is up to $1 million per company.

For more information, please contact Robert M. Wolin, rwolin@bakerlaw.com or 713.646.1327.

OIG OKs FREE BLOOD PRESSURE SCREENINGS

Many hospitals, clinics and other healthcare providers sponsor community health screening events to raise awareness of personal health issues and to provide information on available healthcare services. The Medicare or Medicaid programs, however, limit providers the free items and services that can be provided to beneficiaries.

OIG Advisory Opinion 09-11 analyzed a free screening program under which a small, county-owned critical access hospital would provide free blood pressure checks for any visitor to the hospital who requested one. Screened visitors would not be directed by hospital staff or administrators to utilize the services of any particular healthcare practitioner or provider. No special discounts were offered on follow-up services. If a screened visitor has an abnormal blood pressure reading, the visitor will be advised to see his or her own healthcare professional or, if clinical circumstances demand, the visitor may be directed to an emergency room for an emergency examination.

In the Advisory Opinion, the OIG concluded that free screenings were permissible. The OIG also noted that the free blood pressure checks would fall within a regulatory exception implementing the Civil Monetary Penalties (CMP) statute that allows incentives to be offered to individuals to promote the delivery of preventative care.

Practitioners or providers that participate in Medicare or Medicaid or other federal healthcare programs must structure carefully free community health screenings to (1) satisfy an exception to the CMP, such as incentives offered to promote preventative care; (2) avoid tying the free service to other services offered by the practitioner or provider; and (3) refrain from directing the individual to any particular practitioner or provider, including incentives or discounts on follow-up services, or offering to make appointments with the provider’s own affiliated practitioners. Participants needing follow-up care should be directed to see their own practitioner or provider.

For more information, please contact John S. Mulhollan, jmulhollan@bakerlaw.com or 216.861.7484.

HEALTHCARE TEAM MEMBERS NAMED TO BEST LAWYERS LIST

Seven members of the Baker Hostetler Healthcare Team have been selected for inclusion in the 2010 edition of *The Best Lawyers in America*. They are:

- Donna S. Clark — Houston
- Steven A. Eisenberg — Cleveland
In addition, Baker Hostetler was ranked number one in Healthcare Law for Houston, based on the number of lawyers on the 2010 Best Lawyers roster.

The Best Lawyers list is compiled through an exhaustive peer-review survey in which more than 24,000 of the top attorneys in the U.S. confidentially evaluate their professional peers. The current edition is based on more than 2.8 million votes by these attorneys regarding the legal abilities of other lawyers in the same and related specialties.

**EVENTS CALENDAR**

**September 18**

Houston partner Susan Feigin Harris will present "Healthcare Reform: A Study in Policy, Politics and a Sign of the Times" to the Healthcare Financial Management Association -- Texas Gulf Coast Chapter in Houston, Texas.

Cleveland partner Steven Eisenberg will speak on "From LeBron to Shaq: Expanding the Footprint of an Integrated Delivery System Through a Strategic Growth Plan" at the Ohio Hospital Association 2009 Fall Conference and Annual Meeting in Newark, Ohio.

**September 22**

Columbus and Orlando partner Rick Siehl will present "Legal Implications of Wellness Programs" to the Healthy Ohio Business Council at the OhioHealth Westerville Campus in Westerville, Ohio.

**October 12**

Houston partner Scott McBride will present "The Torture RAC: Managing Overpayment Issues and Disputes" at the Texas Health Law Conference sponsored by the State Bar of Texas and Texas Hospital Association in Austin, Texas.

**October 13**

Houston partner Donna Clark will speak on "Fraud and Abuse and Stark Law Update" at the Texas Health Law Conference sponsored by the State Bar of Texas and Texas Hospital Association in Austin, Texas.

---

**About Baker Hostetler’s National Healthcare Team**

Baker Hostetler is at the forefront of national law firms providing clients involved in every facet of healthcare delivery across the country with comprehensive legal counsel of remarkable responsiveness, creativity, quality and value. We understand the unique needs of the industry, and are dedicated to helping clients achieve their strategic and operational goals and resolve day-to-day operating issues through our experience, knowledge and national perspective. Supported by more than 600 attorneys and professionals in 10 cities coast to coast, our multi-disciplinary Healthcare Team offers clients nationwide strength across a diverse array of practice areas including Medicare and Medicaid reimbursement, regulatory compliance, fraud and abuse counseling, government investigations, subpoenas and audits, FDA, pharmaceuticals and biotechnology, tax and exempt organization laws, export controls, ERISA, management labor and employment, finance and business transactions, antitrust, lobbying, and commercial litigation, among others.

Baker & Hostetler LLP publications are intended to inform our clients and other friends of the Firm about current legal developments of general interest. They should not be construed as legal advice, and readers should not act upon the information contained in these publications without professional counsel. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you written information about our qualifications and experience. © 2009 Baker & Hostetler LLP