

# Health Law ADVISORY

*Current legal insights for health care executives*

July 31, 2008  
Julie A. Knutson, Editor

## *Health Care Organizations and Compliance with the FTC's New "Red Flag" Regulations*

Beginning in November, health care providers may be required to comply with new federal regulations aimed at curbing identity theft. The rules, adopted by the Federal Trade Commission earlier this year, implement the Fair and Accurate Credit Transactions Act and require that covered companies establish programs to address potential identity-theft "red flags."

Because the new rules employ broad definitions that extend to non-bank "creditors" and businesses that make deferred-payment sales, any health care provider that establishes consumer or business accounts for recurring payments may be required to establish procedures to prevent identity theft. Whether your organization must comply hinges on whether it maintains "covered accounts," which are defined as: (1) accounts designed primarily for personal, family, or household purposes that involve or permit multiple payments or transactions; or (2) any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft. Your organization should conduct a review of all accounts to determine whether you may be covered by this rule.

### **Elements of an Identity Theft Prevention Program**

Companies covered by the new rules must establish identity theft prevention programs designed to "detect, prevent and mitigate" identity theft. To this end, the rules include four major requirements.

- 1. Programs must be tailored to potential risks.** Under the new rules, each creditor must assess whether a program is necessary to protect any covered accounts. If the organization determines that a program is necessary, it must establish a written program tailored to the risks facing its accounts.
- 2. Programs must be designed to identify and detect "red flags."** Covered organizations must attempt to identify and detect "red flags." A red flag is "a pattern, practice, or specific activity that indicates the possible existence of identity theft." For example, your health organization could be at risk of identity theft for the purpose of obtaining medical services. If so, your organization must identify red flags that reflect this risk.

### **ALSO IN THIS ISSUE**

- Joint Commission Issues Sentinel Event Alert Targeting Disruptive Physicians 2
- OIG Approves the Issuance of \$10 Gift Cards through a Properly Structured Customer Relations Program 3
- Providence Health Agrees to Pay \$100,000 For Alleged HIPAA Privacy and Security Breaches 5
- Upcoming Speaking Engagements 6

**Find back issues of our newsletters at: [www.bairdholm.com/subpages/newsletters.aspx](http://www.bairdholm.com/subpages/newsletters.aspx)**

**3. Programs must respond appropriately to red flags.**

Procedures to detect red flags may include procedures for detecting suspicious transactions, authenticating customer identities, and verifying address changes. When red flags are detected, the program should provide for appropriate responses, such as contacting affected customers, monitoring affected accounts, or notifying law enforcement.

**4. Programs must be appropriately administered and periodically updated.**

Covered organizations must periodically review and update their programs to address new risks and changed circumstances. They also must ensure oversight of the program and provide appropriate staff training.

**Examples of identity-theft “red flags” common to health care providers**

- Presentation of suspicious documents: Social Security or Medicare cards are the same as those submitted by other account holders or customers;
- Presentation of suspicious personal identifying information: A Social Security Number has not been issued or is listed on the Social Security Administration’s Death Master File;
- Suspicious activity related to a covered account: A suspicious address change is made to a covered account;
- Alerts from Consumer Reporting Agencies: A credit reporting agency provides a notice of credit freeze in response to a request for a credit report.

# *Joint Commission Issues Sentinel Event Alert Targeting Disruptive Physicians*

A new Leadership standard (LD.03.01) will become effective January 1, 2009. The standard includes two Elements of Performance (EP) directed to disruptive and inappropriate behavior. EP4 requires accredited hospitals to have a code of conduct that defines “acceptable” and “disruptive and inappropriate” conduct. EP5 requires leaders to create and implement a process for managing disruptive and inappropriate behaviors.

In its discussion of the new standard and EPs, the Joint Commission directly links intimidating and disruptive behaviors to medical errors; increased costs of care; decreases in retention of qualified clinicians and administrators; and creation of a cultural influence that undermines safety. The Alert states:

*“[t]o assure quality and to promote a culture of safety, health care organizations must address the problems that threaten the performance of the health care team.”*

Research regarding patient safety and disruptive behavior cited in the Alert indicates that disruptive behavior, unfortunately, is not unusual. A study conducted by the Institute for Safe

*“[t]o assure quality and to promote a culture of safety, health care organizations must address the problems that threaten the performance of the health care team.”*

**Vickie J. Brady  
Jonathan J. Wegner**

Medication Practices showed that as many as 40 percent of clinicians did not speak up or question orders when a “known intimidator” was involved.<sup>1</sup>

The Joint Commission also emphasized the “six core competencies to be renewed in the credentialing process which include the competency of interpersonal skills and professionalism.”

In addition to the two new EPs, the Alert lists eleven additional recommended steps which range from education emphasizing appropriate behavior; zero tolerance for intimidating and disruptive behaviors, including incorporating procedures for addressing such behaviors into Medical Staff Bylaws and administrative policies; steps to encourage reporting of inappropriate behavior and surveillance and inquiry systems to detect behavior that is not reported and addressing mental or physical issues which may underlie inappropriate behavior.

While many hospitals, accredited and non-accredited, may have Codes of Conduct in place, it is clear that the Alert calls upon health care organizations to go beyond a mere statement by:

- Implementing the Code of Conduct with detailed strategies/procedures of interviewing with disruptive practitioners;
- Taking active steps not only to investigate reported disruptive conduct but to encourage reporting and solicit information from staff members.

Even for non-accredited facilities, this is one more call to action to reduce errors and improve the safety and quality of care.

**Julie A. Knutson**

## *OIG Approves the Issuance of \$10 Gift Cards through a Properly Structured Customer Relations Program*

The OIG recently provided guidance whereby it approved what is likely a prevalent activity in the health care industry regarding the issuance of a *de minimis* gift to individual patients who submit minor complaints regarding some element of service. While these types of customer relations programs are most likely already in place at many health care providers as a means of staving off further patient complaints and increasing patient opinions related to the quality of services provided, such arrangements have never received analysis and approval by the OIG as to the implications the federal anti-kickback statute and civil monetary penalties laws on such programs. OIG Advisory Opinion 08-07 (issued June 27, 2008) provides such an analysis. Advisory opinions are only binding between the party seeking the opinion and the OIG. However, they do provide guidance as to how the OIG will view and treat similar arrangements.

Advisory Opinion 08-07 responds to a

*The OIG recently provided guidance whereby it approved what is likely a prevalent activity in the health care industry regarding the issuance of a de minimis gift to individual patients who submit minor complaints regarding some element of service received.*

<sup>1</sup> Institution for Safe Medication Practices. Survey on workplace intimidation 2003. Available online at [https://ismp.org/survey/survey\\_results/survey0311.asp](https://ismp.org/survey/survey_results/survey0311.asp)

health system's plan to provide \$10 gift cards to dissatisfied patients who register a complaint about lackluster service provided by an affiliate of the health system. The proposal set forth that the customer relations program was intended to better manage and resolve patient complaints regarding certain service shortfalls. The complaints that were eligible for the program were not related to the quality of patient care. For example, some of the complaints subject to the program were excessive wait times, cancelled appointments, delayed meals, excess noise, housekeeping or dietary concerns and problems with patient comfort equipment such as televisions or the loss of personal items.

Upon receiving a complaint, the health system would issue a \$10 gift card to the complainant through a third-party gift certificate service. The gift card would be for one of a number of local vendors that were members of the gift certificate service. The gift card would not be redeemable at any affiliates of the health care system or at other vendors of health care items such as pharmacies and durable medical equipment suppliers. The health system was also using a tracking system whereby it could keep track of the aggregate amount of gift cards provided to individual complainants and ensure that the amount would not exceed \$50 annually. Furthermore, the tracking system was going to track the areas in which complaints were most prevalent in order to assist management in the identification of problem areas so it could address the underlying concern and improve the quality of a patient's experience while receiving services at an affiliate of the health system. Finally, the customer relations program would not be advertised or used to increase the number of patients receiving services at the health system.

The OIG ultimately approved this

customer relations program because it determined it did not pose a risk of increased usage of items or service paid for by a Federal health care program. The individual gift cards would not have a value of over \$10 and individual complainants would not be eligible to receive more than \$50 in gift cards for the entire year. This was well within the definition of "nominal value" set forth by the OIG in previous guidance. Furthermore, the OIG opined that there was no risk because the gift cards would only be redeemable at non-health care vendors and not at vendors selling items or services reimbursable by a Federal health care program or affiliates of the health system. Based upon all of these facts, the OIG decided that the customer relations program as proposed would not violate the federal anti-kickback statute or result in civil monetary penalties being assessed against the health system.

Advisory Opinion 08-07 should serve as a reminder to hospitals and health systems providing similar incentives that such programs must be structured to ensure that they are compliant with federal law and do not risk the imposition of sanctions under the federal anti-kickback statute or civil monetary penalties laws.

**Andrew D. Kloeckner**

*The OIG ultimately approved of this customer relations program because it determined it did not pose a risk of increased usage of items or service paid for by a Federal health care program.*

# *Providence Health Agrees to Pay \$100,000 For Alleged HIPAA Privacy and Security Breaches*

On July 17, 2008, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) and the Centers for Medicare and Medicaid Services (CMS) jointly entered into a Resolution Agreement with Seattle-based Providence Health and Services (Providence). Providence agreed to pay a voluntary settlement of \$100,000 to resolve HIPAA privacy and security allegations and implement a detailed corrective action plan. The Providence settlement marks the first monetary settlement entered into by a covered entity since the HIPAA Privacy Rule took effect in 2003. Importantly, Providence did not admit any violations of HIPAA and thus the settlement was structured as a “resolution payment” to avoid an actual assessment of civil monetary penalties under HIPAA.

The alleged breaches of privacy and security involved two Providence entities, Providence Home and Community Services and Providence Hospice and Home Care. In 2005 and 2006, as part of Providence’s data backup protocol system, employees took laptop computers home for “safekeeping.” Backup tapes and laptop computers containing unencrypted,

individually-identifiable health information were subsequently stolen, in one instance, from an employee’s vehicle. Four additional incidents involving unattended or stolen laptops were alleged. Providence publicized the loss of the laptops and other sensitive items and informed the 386,000 affected patients of the thefts. As part of a settlement agreement with the State of Oregon, Providence agreed to provide the affected patients with free credit monitoring and to increase data security measures.

The Resolution Agreement provides that Providence will enter into a corrective action plan to ensure that Providence appropriately safeguards identifiable electronic protected health information against theft or loss. The corrective action plan is effective for three years and, among other very stringent requirements, calls for Providence to submit copies of written policies and procedures to HHS for approval. Providence also must submit to HHS a one-time implementation report and annual reports for three years detailing compliance with the policies and procedures adopted as part of the Resolution Agreement.

To date, OCR and CMS have resolved around 6,700 cases, but have not imposed any civil monetary penalties for violations of HIPAA privacy and security rules. The Providence settlement sends a strong signal that OCR and CMS are beginning to take a stronger position against HIPAA privacy and security incidents. The Identity Theft Resource Center reports that there has been a 68% increase in data breaches in the past year, with 39% related to the loss of devices. Health care entities have been in the spotlight with high profile security breaches, which has resulted in a significant focus by CMS on HIPAA privacy and security compliance. The acting Administrator of CMS commented that, “This [Providence] resolution confirms that

*To date, OCR and CMS have resolved around 6,700 cases, but have not imposed any civil monetary penalties for violations of HIPAA privacy and security rules.*

effective compliance means more than just having written policies and procedures. To protect the privacy and security of patient information, covered entities need to continuously monitor the details of their execution, and ensure that these efforts include effective privacy and security staffing, employee training and physical and technical features.” In addition to written policies, organizations should examine the execution of procedures to detect any vulnerabilities in your HIPAA privacy and security compliance system.

While the Providence resolution highlights poor security processes at Providence, it does not take an actual security breach to put an organization under CMS’ scrutiny. In the April edition of the Health Law Advisory, we alerted you to the Sample Interview and Document Request for HIPAA Security Investigations and On-site Compliance Reviews document published by CMS. If you have not yet begun your self-analysis using this sample document as a starting point for measuring your compliance, you should do so now. CMS has hired Price Waterhouse Coopers to assist them in the development of a security audit process for conducting on-site HIPAA compliance reviews. They have announced that 20 compliance reviews will be completed in 2008, although we are not yet aware of any such on-going audits. First up will be covered entities with HIPAA security complaints having been filed, but eventually CMS will reach all covered entities with an on-site compliance review. Are you ready?

**Vickie J. Brady**  
**Michael W. Chase**

## Upcoming Speaking Engagements

Barbara Person will present “Untangling the Web of Ethnic Diversity: Language, Dual Identities, Aliases and Undocumented Workers” at the Iowa AAHAM on September 11, 2008 in Des Moines/Johnston, Iowa and at the Nebraska AAHAM on September 18, 2008 in Grand Island, Nebraska.

**BAIRD HOLM** <sup>LLP</sup>  
ATTORNEYS AT LAW

### HEALTH CARE GROUP

**Vickie J. Brady**

402.636.8230

vbrady@bairdholm.com

**Alex (Kelly) M. Clarke**

402.636.8204

kclarke@bairdholm.com

**John R. Holdenried**

402.636.8201

jholdenried@bairdholm.com

**Andrew D. Kloeckner**

40.636.8222

akloeckner@bairdholm.com

**Julie A. Knutson**

40.636.8327

jknutson@bairdholm.com

**Barbara E. Person**

402.636.8224

bperson@bairdholm.com

*All attorneys are admitted to practice in  
Nebraska and Iowa.*

MEMBER

**LEX MUNDI**

THE WORLD'S LEADING ASSOCIATION OF INDEPENDENT LAW FIRMS

*Health Law Advisory* is intended for distribution to our clients and to others who have asked to be on our distribution list. If you wish to be removed from the distribution list, please notify [healthupdate@bairdholm.com](mailto:healthupdate@bairdholm.com).

**BAIRD HOLM LLP**

1500 Woodmen Tower

Omaha, NE 68102

402.344.0500

402.344.0588

[www.bairdholm.com](http://www.bairdholm.com)

©2008 Baird Holm LLP