CCH Health Care Compliance LETTER

Volume 11, Issue 9 health.cch.com April 29, 2008

OIG refines self-disclosure protocol requirements

Providers that make appropriate disclosures under the Office of Inspector General's (OIG's) self-disclosure protocol (SDP) will have the benefit of a presumption against imposition of corporate integrity agreements (CIAs) or certification of compliance agreements (CCAs), according to an open letter to health care providers issued by Inspector General Daniel R. Levinson on April 15, 2008. The letter, which refines the requirements for participation in the SDP, "emphasizes the OIG's commitment to streamline its internal process for self-disclosure case resolution," the OIG said in a related press release.

The SDP provides guidance to health care providers that voluntarily disclose fraudulent conduct affecting Medicare, Medicaid, and other federally funded health care programs, including compliance issues that the provider believes potentially violate federal criminal, civil, or administrative laws for which exclusion or civil monetary penalties may be imposed.

CIAs and CCAs. According to the open letter, providers that disclose in good faith, cooperate with the OIG, and promptly provide requested information will not be required to enter into CIAs or CCAs with the OIG.

"A provider's submission of a complete and informative disclosure, quick response to OIG's requests for further information, and performance of an accurate audit are indications that the provider has adopted effective compliance measures," Levinson explained. "We believe that this presumption in favor of not requiring a compliance agreement appropriately recognizes the provider's commitment to integrity and also advances our goal of expediting the resolution of self-disclosures," he added.

Additional requirements. For a provider to participate in the SDP and benefit from the presumption in favor of not requiring CIAs and CCAs, the initial submission to the OIG must contain:

(1) a complete description of the conduct being disclosed;
(2) a description of the provider's internal investigation or a commitment regarding when it will be completed;
(3) an estimate of the damages to the federal health care programs, along with an explanation of the methodology used to calculate the estimate, or a commitment regarding when the estimate will be completed; and
(4) a statement of the laws potentially violated by the conduct.

This information must be included in addition to the basic information described in the SDP. The provider must be in a position to complete the investigation and damages assessment within three months after acceptance into the SDP.

Levinson emphasized in the open letter that the "refinements to OIG's SDP process are intended to provide an opportunity for providers to work with OIG to more efficiently and fairly resolve matters appropriately disclosed under the SDP.... [T]his approach benefits both disclosing providers and the [g]overnment and furthers our efforts to strengthen the integrity of the [f]ederal health care programs." ■

OIG Press Release April 15, 2008; Open Letter to Health Care Providers, April 15, 2008, Health Care Compliance Reporter ¶530,666.

Wolters Kluwer Law & Business

IRS Form 990 draft instructions provide practical guidance

Draft instructions for the Internal Revenue Service (IRS) 2008 Form 990, Return of Organization Exempt from Income Tax, "provide some much needed clarification to those that exist now," according to Greg Goller, partner in charge of Grant Thornton LLP's not-for-profit tax practice. "For example, ratable reporting of nonvested deferred compensation...seems reasonble to me. The draft instructions also seem to increase awareness of the rules by providing practical guidance about particular areas of tax compliance. For example, political activities include those conducted by disregarded entities or entities taxed as partnerships," he added.

The redesigned Form 990—the annual return most tax-exempt organizations will be required to use to report information about their operations—was released in final form in December 2007 without instructions. The draft instructions are for the Form 990 that organizations will file for their 2008 tax year (returns filed in 2009).

New tools. The draft instructions provide a general overview of the Form 990 and its schedules, an explanation of which organizations must file a particular schedule, and line-by-line instructions on how to answer each question on the form or schedule. The draft instructions also contain a number of new tools designed to make it easier for tax-exempt organizations to answer the questions and to promote more consistent reporting.

The tools include, among others: a comprehensive glossary of terms; a sequencing list to help organizations determine the order in which to fill out parts of the form; and a compensation table to help organizations determine how and where to report items of compensation. "The compensation table will help organizations determine how to identify, classify, and properly report many of the different elements of current and deferred compensation as well as fringe benefits," Goller said

FIN 48 footnote. In Schedule D, Supplemental Financial Statements, the IRS requires organizations to provide a FIN 48 (Financial Accounting Standard Board's Interpretation 48, Accounting for Uncertainty in Income Taxes) footnote regarding liability for uncertain tax positions. Organizations that file financial statements as part of a consolidated group are only required to provide a footnote for information pertaining specifically to the organization, according to Stephen Clarke, Tax Law Specialist, IRS Tax Exempt and Government Entities Division.

Hospitals. New Schedule H, Hospitals, will be phased in over time, Clarke noted. Only Part V, Facility Information, has to be completed in 2008. The instructions will define the term "facility" and address who should file Schedule H. According to Clarke, the IRS wants to know more about hospitals' activities. "We are especially interested in knowing whether the definitions of hospital, facility, and community benefit are appropriate."

Compensation. There are extensive instructions as to what is deferred compensation in Schedule J, Compensation Information, Clarke observed. He reported the IRS' interest in whether compensation is treated appropriately in Schedule J. He also referred to the compensation matrix provided by the IRS, which instructs organizations where to report compensation.

Key employees. The IRS has proposed an expanded definition of the term "key employees," which Goller believes "will likely increase the list of persons reported in Part VII of the core form." Key employees may now include individuals who "manage or have authority to control" more than 5 percent of the organization's activities, assets, income, expenses, capital expenditures, operating budget, or compensation of employees if they earn over $150,000. "I'd suggest a higher percentage than 5 percent and more clarification as to the definition of 'manage' and 'has or shares the authority to control,'" he added.

Other significant changes. With respect to the scope of significant changes to governing documents (*i.e.*, articles of incorporation and bylaws), Clarke explained that the IRS is only interested in significant changes, such as changes to qualifications or duties of board members. He emphasized that the IRS would not be interested in changes to the number of committee meetings per year, for example, which would not be a significant change. Clarke noted that examples are provided in the instructions. Significant changes should be described in schedule O, Supplemental Information to Form 990, but the articles and bylaws

continued on page 3

CCH Health Care Compliance Letter

Portfolio Managing Editor
Pamela K. Carron, J.D., LL.M

Coordinating Editors
Susan Smith, J.D., M.A.
Matthew Mann, J.D.
Valerie Witmer, J.D.

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard, M.A.
Tax–Jeff Carlson, Steve Cooper, Chandra Walker

Designer
Laila Gaidulis

Requests for information about article submission and comments from readers are welcome and should be directed to Susan Smith at susan.smith@wolterskluwer.com, Tel. 847-267-2780, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Health Care Compliance Letter is published 24 times a year by CCH, a Wolters Kluwer business, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

should not be attached unless the organization changes its name, he said.

Public comment. The IRS is soliciting comments on the draft instructions and has extended the comment period through June 1, 2008. Clarke urged tax-exempt organizations to focus on the highlighted sections of the instructions, which represent significant changes or areas in which the IRS is particularly interested in receiving comments. He observed that the 2008 instructions are lengthier than the 2007 instructions.

The IRS is seeking comments from the tax-exempt community in an effort to make sure the final instructions meet the needs of exempt organizations. "Comments are extremely helpful and we view the Form 990 redesign project as a collaboration between the sector and the IRS," Clarke emphasized.

Clarke noted that the IRS anticipates publishing the instructions in final form by the end of 2008. ■

CCH Washington Bureau, April 7-8, 2008.

PQRI options include registry-based reporting, new reporting periods

New reporting options "will make it easier for eligible professionals to participate in the [Physician Quality Reporting Initiative (PQRI)] and receive feedback on their performance," according to CMS. In late 2007, Congress made changes to the PQRI with the passage of the Medicare, Medicaid, and SCHIP Extension Act (PubLNo 110-173) (Extension Act), which provided new flexibility for submitting data and implemented registry-based reporting. These changes "will ultimately improve the services provided...[b]y providing more opportunities to submit information about the quality of care provided to Medicare beneficiaries," CMS Acting Administrator Kerry Weems said.

2008 PQRI program. Implemented in 2007, the PQRI creates a quality reporting system that includes an incentive payment for satisfactorily reporting data on quality measures for covered professional services provided to Medicare beneficiaries. The 2008 PQRI program allows the use of 119 quality measures that were included in the Medicare physician fee schedule for calendar year 2008. Of those measures, 117 are clinical performance measures, such as the percentage of patients who received necessary cancer screenings and flu shots, and two are structural measures. The structural measures focus on the use of electronic health records and electronic prescribing technology.

New reporting options. The Extension Act authorized PQRI transitional bonus payments in 2008 without the cap that applied to incentive payments in 2007. It also required the Secretary of HHS to establish alternative criteria and reporting periods for both the reporting of groups of measures and the use of registry-based reporting.

For 2008, in addition to submitting PQRI data as part of their Medicare claims submissions, eligible professionals may report data on quality measures to a medical registry, which will report that data to CMS. "[R]egistry-based reporting will provide more ways for eligible professionals to qualify for an incentive payment," CMS noted.

Another change under the 2008 PQRI is new reporting periods for eligible professionals who report using measures groups. Participants may now start reporting in July 2008 and be eligible to earn an incentive payment for the 2008 PQRI program.

Participation data. Preliminary participation data indicates that the program has been successful. CMS believes that more than half of the 100,000 professionals who submitted PQRI data at least once in 2007 will receive an incentive payment. "We are encouraged by the success of the program so far, and with the new options for data reporting, more health professionals should take advantage of the reporting program," Weems said. He added, "These new options will help all health care stakeholders take the positive steps necessary to ensure that beneficiaries continue to get high quality care." ■

CMS Press Release, April 17, 2008.

HIPAA privacy and security rule update: Tougher enforcement expected in 2008

by Laura J. Merisalo, Contributing Editor

This month marks the fifth year of enforcement of the Health Insurance Portability and Accountability Act (HIPAA) privacy rule, and the third year of enforcement of the HIPAA security rule, each of which has patient access implications.

The privacy rule serves to safeguard the confidentiality of individually identifiable health information in any format, while the security rule sets standards to protect health information in electronic format. Each rule has implications for patient access, as front-end employees daily manage patients' personal and private health information.

As these enforcement anniversaries are notched, so will HIPAA enforcement be stepped up in 2008. This year, CMS contracted with PricewaterhouseCoopers to conduct security rule audits at up to 20 organizations through September 2008. This contract comes on the heels of a security rule audit quietly launched in March 2007 at iedmont Hospital in Atlanta.

HHS' commitment to enforcement of the privacy rule was revealed with the April 2007 launch of its Health Information Privacy Web site. This Web site provides information for health care providers, consumers, health plans, and others regarding HHS compliance and enforcement efforts. The Web site also provides current data on enforcement efforts, which shows that the number of investigated resolutions increased by more than 600 percent within the first three years of privacy rule compliance.

Compliance is dynamic

Although health care organizations have adopted policies and procedures to ensure compliance with the HIPAA privacy and security rules and provided related staff training and education to employees, the work of compliance does not end with implementing new processes and training employees on the new ways of working. Rather, compliance is a dynamic affair. It requires ongoing monitoring, training and tweaking to identify and manage potential risks and ensure that the purpose and goals of compliance are achieved.

Patient access employees' responsibility to comply with policies and procedures to protect patient privacy is significant, as patient access employees are people in trust relationships, William M. Miaoulis, a consulting manager and HIPAA service line leader with Phoenix Health Systems notes. Patients trust that personal information shared with patient access employees goes no further than the employee conducting the registration interview, and that it stays with their patient record to be used as appropriate by the physicians, nurses, and other clinical staff members involved in their medical care.

To ensure HIPAA compliance, Miaoulis says, training must be supported by monitoring. "If you are monitoring and find [employees] are doing the right things, then you know your training is good. If you find lapses, then you need to intervene and do more training."

Medical identity theft coverage

Compliance with the HIPAA privacy and security rules has significance beyond staying in step with federal law. Adhering to standards and requirements under the HIPAA privacy and security rules also serves to combat another major issue cited as one of the fastest growing crimes in America—identity theft. In health care, medical identity theft wreaks havoc on all involved: patients, providers, payers, and even perpetrators posing as patients whose identities they have stolen may become unwitting victims in medical identity theft.

As the health care industry increasingly relies upon electronic data and documentation for all aspects of a health care encounter, the risk of unauthorized access to such information also increases. The 80–20 rule applies to this risk, according to industry experts, with the greatest risk of unauthorized access to protected health information most likely to come from within an organization rather than from external sources or hackers.

In the health care industry, medical identity theft evolves into health care fraud through unauthorized use of patient names, insurance cards, and Social Security numbers to gain access to coverage for medical care by posing as another person. Potential damages may extend beyond instances of fraud related to specific health care encounters, however, and may include credit theft, discrimination, employment issues, and delivery of inappropriate health care, which could have tragic, even life-threatening, consequences.

Medical identity theft presents the potential for serious personal health risk for the patient whose identity is stolen as well as the person who uses a stolen medical identity to receive health care. For patients whose medical identities are stolen, their medical records may end up containing faulty information that is incorporated into their medical records based on treatments or diagnoses of the identify thieves. For

medical identity thieves, the personal health risk includes that the medical history of the real patient is relied upon for their treatment, and it will not reflect the medical conditions of the identity thief.

Thus, it is imperative health care provider organizations ensure that individuals' personal health information is safe and secure for a number of reasons, including to protect patient privacy and to avert the risk of medical identity theft and the host of ensuing potential consequences.

Privacy versus security

The HIPAA privacy and security rules are different, but "they work together like hand and glove," Miaoulis explains. Most simply, he says, "the privacy rule gives [patients] rights, and the security rule is how you help ensure privacy."

The privacy rule, effective in April 2003, sets standards to ensure the protection of protected health information (PHI) in all forms—whether electronic, written, or oral. In addition to protecting patients' health information, the privacy rule also sets standards that serve to provide patients with access to their medical records and more control over how their personal health information is used and disclosed. The privacy rule is enforced by the HHS Office for Civil Rights (OCR).

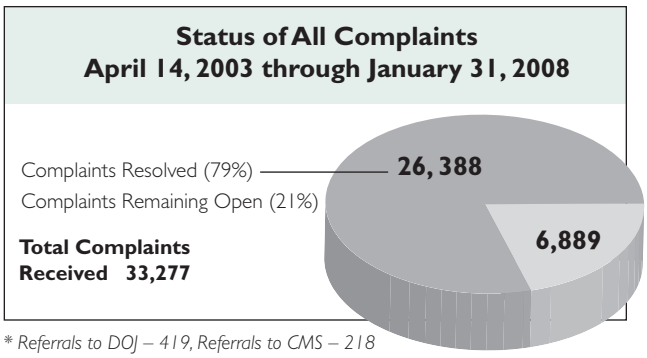
The privacy rule requires that covered entities have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."[1] Miaoulis notes that privacy rule compliance requires that organizations take "reasonable" measures to ensure that patients' private health information is protected. For instance, when the privacy rule first took effect, there was concern regarding whether sign-in logs could be used at patient access, Miaoulis says. When this concern was placed into context with what is reasonable, the sign-in log itself proved not to be objectionable so long as the log excluded any private health information, such as diagnosis codes or reasons for a patient's visit, that could be publicly viewed by those using the sign-in log.

The security rule, effective in April 2005, sets forth standards to ensure that electronic protected health information (EPHI) is indeed protected, with enforcement by CMS. The security rule covers EPHI that is created, received, maintained, or transmitted over the Internet, on a computer, or via a CD, disk, magnetic tape or other electronic means.

Although every aspect of the HIPAA privacy and security rules may not require a specific and corresponding patient access response or process, Miaoulis notes, patient access professionals still must understand the rules and related compliance standards. "Patient access needs to understand the [privacy and security rule] processes that may not be theirs to do, but they need to be able to direct people" when questions or issues related to protected health information arise.

For example, Miaoulis says, patient access employees may field patient requests for medical records, but patient access is not the source for such information or documents. Still, front-end employees need to: (1) understand that patients are within their rights to request access to their personal medical information; and (2) respond by directing patients to the appropriate department.

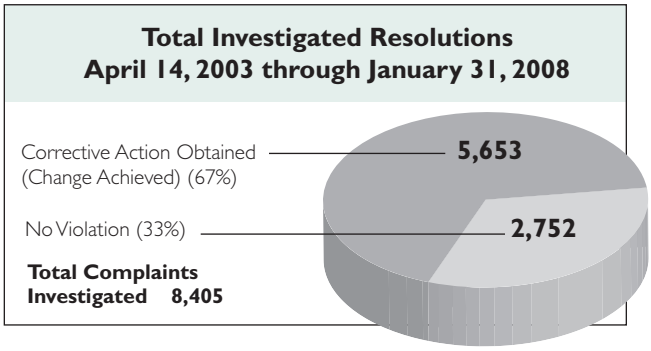
Exhibit 1



** Referrals to DOJ – 419, Referrals to CMS – 218*

Source: Department of Health and Human Services, Office of Civil Rights, HIPAA Compliance and Enforcement, February 2008.

Exhibit 2



Source: Department of Health and Human Services, Office of Civil Rights, HIPAA Compliance and Enforcement, February 2008.

Privacy rule enforcement highlights

Since compliance with the privacy rule took effect five years ago, the OCR has received 33,277 complaints of alleged privacy rule violations, from April 14, 2003, through January 2008. (see Exhibit 1). Of those complaints, 21 percent, or 6,889, remain open, and 79 percent, or 26,388, have been resolved. Of the resolved complaints:

- 17,983 were resolved by closure after the complaints were found not to be eligible for enforcement due to the OCR's lack of jurisdiction under HIPAA, the complaints were untimely, withdrawn, or not pursued by the filer, or the activity described did not violate the privacy rule;[2]
- 8,405 were investigated, with 67 percent, or 5,653, requiring corrective action (see Exhibit 2); and
  33 percent of investigated complaints, or 2,752, were not violations (see Exhibit 2).

Since compliance began in 2003, the number of complaints investigated has increased significantly each year, from a total of 339 complaints investigated in 2003, to 2,466 complaints investigated in 2006. That represents a 627 percent increase within the first three years. (see Exhibit 3).

Complaints of HIPAA privacy rule violations since April 2003 have included 5,653 cases that required changes in privacy practices and other corrective actions by the covered entities. The corrective actions have included requiring systemic changes in privacy practices, as well as changes that affect individuals served by the covered entity.

Health care provider organizations make up the top three of the five covered entity types most frequently found in violation of the privacy rule.[3] The top three covered entities most frequently found in violation of the privacy rule, in order, are: private practices, general hospitals, and outpatient facilities.[4] Health plans and pharmacies ranked fourth and fifth, respectively, in frequency of violation findings.[5]

Privacy rule violations investigated most often fall into five categories. These categories, in order of frequency, include:

(1) impermissible uses and disclosures of protected health information;
(2) lack of safeguards for protected health information;
(3) lack of patient access to protected health information;
(4) uses or disclosure of more than the minimum necessary protected health information; and
(5) lack of or invalid authorizations for uses and disclosure of protected health information.[6]

Privacy rule at patient access

A key provision of the privacy rule requires that patients be provided with a notice of a provider's privacy practices and patients' rights to access private health information. This provision falls to patient access and requires front-end processes that accomplish the following:

- On or before the first date of service, patients must be provided notice of a provider's privacy practices and notified of their individual privacy rights. The notice of privacy practices outlines patients' rights to access their protected health information, as well as the institution's obligations to protect private health information. The notice also outlines how patients' medical information may be used and disclosed by law or patient permission.
- Patient access must obtain patients' written acknowledgement of receipt of the notice of privacy practices and patients' rights, or document "good faith effort" made to obtain written acknowledgement.
- If the initial patient contact is by telephone, the privacy rule allows for providers to meet the privacy notice requirements when the patient arrives for the service.
- The privacy notice must be provided to anyone who asks for it, not just patients. It also must be prominently posted and available on Web sites that provide information about customer services or benefits.
- If the initial patient encounter is electronic, through online scheduling, for instance, the privacy rule requires that the electronic notice be sent "automatically and contemporaneously" in response to the patient's service request. An electronic return receipt from the patient is considered valid written acknowledgement of the privacy notice.
- Emergency medical care and treatment are the exceptions to the first date of service requirement for when patients are to be provided the notice of privacy practices and patient rights. In emergency situations, providers must give patients the privacy notice as soon as reasonably practical, after the emergency situation is resolved.

The privacy rule also mandates that employees have authorized access only to the minimum necessary patient health information. The minimum necessary caveat requires that registration employees have access to information needed to verify a patient's identity, which may include information about previous visits, Miaoulis says, "but the actual clinical information about previous visits is not necessary at patient access."

Security enforcement

The first security audit, of the Atlanta-based Piedmont Hospital, was conducted quietly but sent a loud signal that security rule enforcement is an HHS priority. Under the CMS contract with PricewaterhouseCoopers, up to 20 organizations are expected to undergo security rule audits by the end of September. The first to be audited will be institutions against which complaints have been lodged.

The most common security complaints relate to information access management, security awareness and training, access control, workstation use, and device and media controls. Although Piedmont and HHS were tight-lipped about the audit, Computerworld surfaced a document that showed Piedmont was directed to provide within 10 days information on 42 separate items.[7]

This list of items gives health care provider organizations insight into areas of scrutiny that should receive careful attention from patient access and other leaders within the organization. Of HHS interest in the Piedmont audit were policies and procedures for:

- establishing and terminating users' access to systems housing electronic patient health information;
- inactive computer sessions;
- employee violations (sanctions);
- preventing, detecting, containing, and correcting security violations (incident reports);
- regularly reviewing records of information system activity;
- establishing security access controls (what types of security access controls are currently implemented or installed in hospitals' databases that house EPHI data);
- remote access activity;
- Internet usage;
- wireless security (transmission and usage);
- transmitting of EPHI; and
- password and server configurations.

HHS also had more than a dozen other concerns. Auditors requested that Piedmont also provide, among other things:

- a list of all terminated employees and new hires;
- a list of authentication methods used to identify users authorized to access EPHI;
- a list of transmission methods used to transmit EPHI over an electronic communications network;
- a list of all users with access to EPHI data, as well as each user's access rights and privileges; and
- a list of authentication approaches used to verify that a person has been authorized for specific access privileges to information and information systems.[8]

Training, plus monitoring

As HIPAA enforcement efforts are stepped up, patient access leaders need to proactively ensure that front-end employees understand their responsibilities with respect to HIPAA compliance. To ensure that patients' personal health information is protected, patient access employees need thorough training on the policies and processes in place to safeguard protected health information. Training needs to be supplemented with ongoing monitoring to ensure that policies and practices are followed.

For example, Miaoulis suggests occasional walk-throughs in patient access work areas to determine if patient paperwork is processed properly or left in view of others, employees log off prior to leaving a work station, or computer terminals are left unattended.

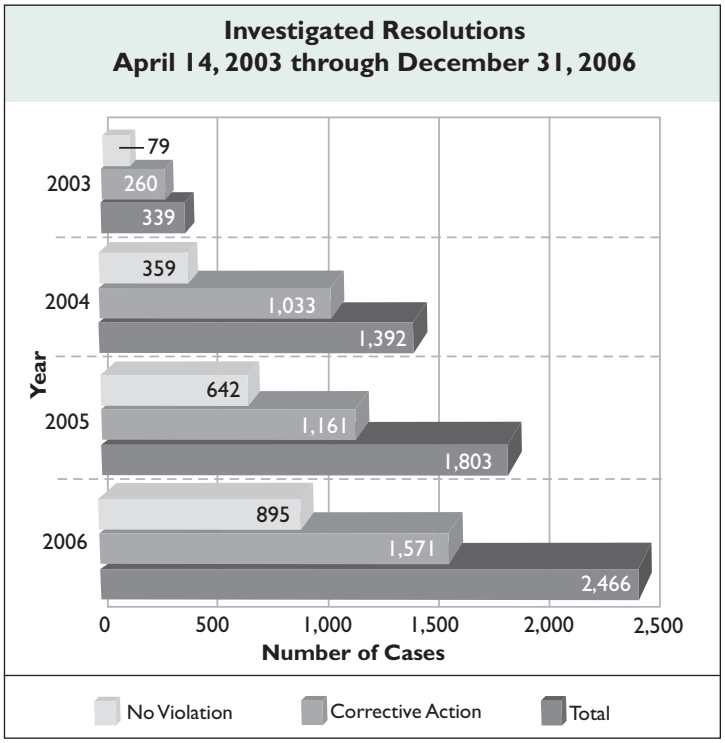
"If I am finding terminals untended...that is a security issue and either my training is not sufficient, or my log-out time is too long," Miaoulis notes. "I then have to identify what my course of action is to improve lack of compliance." As with any process, Miaoulis notes, when issues arise, leaders need to examine the problem area further to identify whether training is adequate or processes need to be revised.

For example, a report that shows the system is initiating automatic log-offs more often than employees are logging off themselves does not necessarily mean employees are lax in leaving computer terminals unattended. The report red flags the issue, and further investigation is needed to determine if employees are not logging off timely and appropriately, or if the automatic log-off period is too short and so is shutting down even as employees are at their work stations.

Miaoulis underscores that it is imperative that patient access professionals receive sufficient training and education so that front-end employees understand the security and privacy rules, as well as patients' rights and the privacy rule compliance mandate. This training is essential to ensure compliance, as well as to ensure employees are able to explain to patients the particulars of the privacy rule.

For example, Miaoulis notes that patient access employees are first in line to explain to hospital inpatients that they have the right to opt out of a hospital's directory. Opting out of the directory means that anyone—including family members—who inquires about the patient will be informed that there is no record of such patient. It is important that patient access professionals are able to clearly articulate to patients just what opting out of the hospital directory means, Miaoulis says. He cites the example of a pregnant woman who opted out of the directory. When the patient arrived at the facility to deliver her baby, her mother was among those with her. The patient's mother left and later returned, only to be told that the hospital has no record of her daughter as a patient, and the mother, not surprisingly, became frantic.

Exhibit 3



Source: Department of Health and Human Services, Office of Civil Rights, HIPAA Compliance and Enforcement, February 2008.

Laura J. Merisalo is editor and principal author of Healthcare Registration, a national newsletter for patient access professionals. Ms. Merisalo also is associate editor for a newsletter on legal issues related to health care reimbursement, contributing editor for a quarterly analysis of hospital accounts receivable, and consulting editor for a comprehensive health care registration manual. She also has served a contributing author for books and manuals on patient access services and revenue cycle management processes. Ms. Merisalo can be reached at hcr@wi.rr.com.

* Reprinted from *Healthcare Registration*, Vol. 17, No. 7, April 2008.

1 See HIPAA privacy rule provisions at 45 C.F.R. §164.530 (c).

2 HHS, Office of Civil Rights, Compliance and Enforcement, Privacy Rule Enforcement Highlights: April 14, 2003, through January 31, 2008.

3 *Id.*

4 *Id.*

5 *Id.*

6 *Id.*

7 Jaikumar Vijayan, *HIPAA audit: The 42 questions HHS might ask*, COMPUTERWORLD, June 19, 2007.

8 *Id.*

Health IT

Senators urge Congress to pass health IT bill

Senate Health, Education, Labor and Pensions Committee leaders urged Congress to consider and pass a bill to expand and standardize information technology (IT) in the health care arena. "We can save thousands of lives and conserve billions of dollars for health care…and we can do it this year," Committee Chairman Ted Kennedy (D-Mass.) said at an April 2, 2008, forum hosted by the Business Roundtable, a Washington D.C.-based association of chief executive officers of U.S. companies.

Kennedy said he hopes the next administration will be able to implement such legislation and end the current stalemate. "The country requires it," he said. He noted that the RAND Corporation has found that widespread use of health IT could produce annual savings in efficiency and improved health outcomes of $165 billion.

Ranking member Mike Enzi (R-Wyo.) added that increased use of health IT would help reduce medical errors and duplicative tests, saving billions of dollars and improving health care. "Moving from a paper-based health care system to secure electronic medical records will save lives and reduce skyrocketing health care costs," he said, adding that "[t]he health care and business communities…are clamoring for Congress to take action and establish uniform health IT standards."

The Wired for Health Care Quality Act (S. 1693) was introduced last June in the Senate. A similar bill—the Promoting Health Information Technology Act (H.R. 3800)—was introduced in the House in October. Both bills would foster implementation of a nationwide interoperable health information network, according to a Business Roundtable release.

"For nearly all businesses, with the notable exception of health care, electronic communication has already moved into second- and third-generation iterations. Yet, today 90 percent of health care records are kept on paper," Ivan Seidenberg, CEO of Verizon Communications and Chairman of the Business Roundtable's Health and Retirement Task Force noted. "Our health care is stuck in time and lacks even the simplest IT foundation," he said in the release. ■

CCH Washington Bureau, April 4, 2008.

In the News

CMS proposes new HIPAA EDI standards

CMS is in the process of implementing the proposed next version of Health Insurance Portability and Accountability Act (HIPAA) electronic data interchange (EDI) transactions—referred to as "HIPAA-2." The administrative simplification provisions of HIPAA require the Secretary of HHS to adopt standard electronic transactions and code sets for administrative health care transactions. The Secretary also may modify these standards periodically. CMS expects to implement HIPAA-2 over four quarterly releases for its shared systems. The intent is for CMS to be ready to accept and send HIPAA-2 transactions in a test environment beginning in the spring of 2009. The results of CMS' comparison of the current HIPAA EDI standards with the proposed standards as used within the Medicare Fee For Service program are now available on the CMS Web site at http://www.cms.hhs.gov/ElectronicBillingEDITrans/18_HIPAA2.asp#TopOfPage.

CMS Web site, April 22, 2008.

Hospital settles FCA allegations for $1.75 million

Touro Infirmary, a New Orleans hospital, has agreed to pay the United States $1.75 million to settle allegations that it submitted false claims to the Medicare program in violation of the Federal False Claims Act, the Department of Justice (DOJ) announced. The United States alleged that between 2000 and 2004, Touro made unlawful payments to a psychiatrist to induce her to refer patients to the hospital. According to the DOJ, the payments were made pursuant to several consultant and medical directorship contracts that were shams intended to disguise kickbacks to the psychiatrist. The United States pursued criminal charges against the psychiatrist, and a jury returned guilty verdicts on 39 counts of health care fraud against her, including 13 counts arising from her contractual relationship with Touro. "Kickbacks are a blight on the health care system," said Jeffrey Bucholtz, Acting Assistant Attorney General for the DOJ's Civil Division. "They corrupt physicians' medical judgment and lead to overutilization and misuse of taxpayer dollars. We will continue to be vigilant in our efforts to combat this pernicious practice."

DOJ Press Release, April 17, 2008.

CMS proposes "stand in the shoes" alternatives

CMS is requesting comments on two alternative proposals to address the "stand in the shoes" provisions described in the Stark Phase III final rule published in the *Federal Register* on September 5, 2007 (72 FR 51012), according to an advance release of the fiscal year 2009 inpatient prospective payment system *Proposed rule*. The first proposal would provide that a physician would be deemed to *not* stand in the shoes of his or her physician organization if the compensation arrangement between the physician organization and the physician satisfies the requirements of the bona fide employment relationship exception, the personal service arrangement exception, or the fair market value compensation exception. The second proposal would make no revisions to the stand in the shoes provisions and, to the extent necessary to protect nonabusive arrangements, promulgate a separate exception for arrangements that are not otherwise covered by existing exceptions.

CMS Release, April 14, 2008, Health Care Compliance Reporter ¶730,036.