Compliance Officer's REPORT

News, tools and best practices to train staff and minimize healthcare legal and regulatory risk.

April 2009 | Vol. 2, No. 4

Dear Reader

When your office or facility contracts with any Medicare Advantage (MA) plan, expect your staff to take the plan's required fraud, abuse and waste compliance training.

This requirement, which became effective Jan. 1, 2009, tells MA plans and Medicare Part D drug plan sponsors to provide the training yearly not only to their own staffs but also to "first tier, downstream and related entities," CMS

(continued on page 3) See Page 3

In This Issue

New stimulus law expands HIPAA privacy and security obligations

Your HIPAA compliance program has just become out-of-date. HIPAA's been amended, and it's now on steroids.

President Obama signed the $787 billion stimulus package, called the American Recovery & Reinvestment Act of 2009 (ARRA), on Feb. 17. It authorizes $19 billion to develop and encourage the adoption of health information technology (HIT) and electronic health records (EHR). To accomplish this, the new law imposes more obligations on providers to protect those records by significantly strengthening HIPAA's privacy and security requirements. Several areas where HIPAA's scope has been expanded include:

- Business associates of covered entities now will be liable under HIPAA for privacy and security breaches. Previously they were only liable for breaching their business associate agreements.
- Providers will have to notify patients, and in some cases the federal government and local media, where there has been a breach of unsecured patient information. Unlike many state laws, which require notification only if unencrypted electronic information is breached, the HIPAA amendment requires notification even if paper records are compromised, and some notifications also will have to go to the Federal Trade Commission.
- Civil monetary penalties have increased, with tiered penalties ranging from $100 to $1.5 million. In addition, employees and other individuals can be found liable under HIPAA. Previously, individuals could not be held liable, although their employers could be held liable for the actions of individuals.
- If they request it, patients can obtain more accounting or explanation of disclosures of their medical record information for purposes of treatment, payment or health care operations. (Previously, disclosures for these purposes were exempt from the accounting requirements.)
- State attorneys general offices have been empowered to enforce HIPAA. Before, only the federal government could do so.

SUBSCRIBER SERVICES

Editorial:

Marla Durben Hirsch, Editor
mhirsch@decisionhealth.com

Richard D. Hadley, Publisher
rhadley@decisionhealth.com

Subscriptions: For direct questions about newsletter delivery and account status, please contact DecisionHealth® at (877) 602-3835, or email us at: customer@decisionhealth.com.

Accuracy: Our goal is to provide you with the most accurate and balanced information available anywhere. If you ever feel we're not living up to this standard, contact Richard D. Hadley directly at 301-287-2257 or rhadley@decisionhealth.com.

Fraud Listserv: To join our free Internet forum on fraud and abuse issues, visit our website at www.decisionhealth.com, click on "discussions" and then "health care facilities, and select "health care fraud and abuse" and "subscribe." Just follow the directions from there.

Reprints: To request permission to make photocopy reprints of *Compliance Officer's Report* articles, or to obtain information on our copyright waiver, multiple copy and site license programs, please call us at (866) 266-1029, or email us at: jwethje@decisionhealth.com.

Compliance Officer's Report (formerly HIPAA Compliance Alert) is published 12 times per year by:

DecisionHealth® (a UCG company)
Two Washingtonian Center
9737 Washingtonian Blvd., Suite 100
Gaithersburg, MD 20878-7364

ISSN: 1941-7764
Price: $419 per year

- The government will be required to conduct more audits to determine HIPAA compliance.
- Covered entities and business associates no longer can sell protected health information in most instances without a patient's authorization.

To review the new stimulus law, go to: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf. The health information provisions run from page 112 to 165.

No RIP for HIPAA

"We thought HIPAA was dead [especially since there hasn't been much enforcement]," says consultant John Parmigiani, Ellicott City, Md., who helped draft the original HIPAA security rule. But HITECH [the part of ARRA that deals with HIPAA] has strengthened the intent of HIPAA and modernized it, he says.

Many of the new requirements will need clarification by new regulations and other guidance from HHS, however. Other provisions are subject to differing interpretations. For instance, it's unclear what constitutes "unsecured" patient information whose breach would trigger the notification requirements and how the federal notification requirement will dovetail with state notification requirements, notes attorney Robin Campbell with Crowell & Moring in Washington, D.C. It's also expected that "health care operations" will soon be defined more narrowly, but it's unknown by how much, adds attorney Barbara Ryland, also with Crowell & Moring.

In addition, it's uncertain whether providers will have to amend all of their business associate agreements (BAAs), and in what way. For instance, if your BAAs already contain a general statement that the business associate will comply with the law, it's unclear whether you'll need to add new language to the BAAs to cover the new amendments. "It's open to debate," says attorney Gerald "Jud" DeLoss, with Gray Plant Moody, Minneapolis.

What is certain, however, is that there will be more enforcement of HIPAA, especially now that state attorneys general can get in on the action. "They're chomping at the bit," says Campbell.

What you should do

The effective dates of the HIPAA amendments vary significantly. Some of the provisions, such as the new penalties and authorization of attorneys general to enforce HIPAA have gone into effect already; others don't go into effect until 2010 or later. There's also doubt if some of the deadlines outlined in the law will be met, since an HHS secretary is

taking office later than anticipated, notes attorney Shirley Morrigan with Foley & Lardner in Los Angeles. "[These changes] will need leadership in terms of the amount of work involved," she explains.

However, providers should take some steps to prepare for these changes:

1. **Get ready to make changes to implement the new HIPAA requirements**, such as updating policies and educating staff about the new provisions, suggests DeLoss. While it's still unclear which specific changes will need to be made, rest assured that you'll have a lot of work to do in the near future.
2. **Assess which business associates you want to continue to work with.** Note that HIPAA now directly applies to them, but many of them aren't used to these laws. You may want to re-evaluate who you work with now that the stakes are higher. "You need to decide if you want to contract with people with repeated breaches," Morrigan says.
3. **Watch for changes in your state laws.** Now that HITECH fills in some of HIPAA's gaps that states had tried to cover, states may modify their own laws to be consistent with the federal law, says Ryland.
4. **Expect ancillary changes from HITECH.** For instance, the law allocates more than $1 billion for "comparative effectiveness research" of health care procedures and products. That may standardize clinical guidelines down the road that your office or facility will need to comply with, says DeLoss.

Compliance Officer's Report will keep you up-to-date regarding new developments.

Dear Reader: MA Plans institute mandatory compliance training

(continued from page 1)

said in an October 2008 memo (www.ascp.com/advocacy/federal/upload/CMS%20FRAUD%20WASTE%20AND%20ABUSE%20TRAINING%20LISTSERVE%20ALERT.pdf). The requirement also was included in a Dec. 5, 2007, HHS regulation that updated the plans' compliance obligations.

Training for your staff will cover measures to detect and prevent fraud, waste and abuse and create effective lines of communication between the plan's compliance officer and others. The preamble to the regulation recommends that the plans obtain training logs and copies of attestation from those it works with to document that training occurred, and that plans consider amending their contracts to require providers to train their workforce.

Each plan must meet the requirement during calendar year 2009. CMS notes in its memo that since providers often contract with many different MA plans, this requirement may impose a burden on providers if they have to take each plan's training. CMS is working with several trade and professional associations to develop a training program that meets CMS' requirements so that providers won't have to take the training multiple times.

MA plans also can develop their own training programs and distribute them to providers. Because the responsibility for MA and Part D training rests with the insurers, physician offices, hospitals and other providers don't have to develop training themselves.

New compliance obligations for HIT incentives

Expect new Medicare requirements as the economic stimulus law (see story, page 1) creates incentives, penalties and new rules regarding the adoption of health information technology (HIT). They accompany the carrot offered in the stimulus package – $17 billion for incentive payments through Medicare and Medicaid to encourage physicians and hospitals to implement electronic health record (EHR) systems by 2015.

Hospitals could potentially receive as much as $11 million in incentives individually; physician practices could get up to $44,000.

After 2015, penalties will be imposed by cutting Medicare reimbursement if a hospital or physician has not become a "meaningful user" of an EHR system that can be used by clinicians and staff across more than one health care organization.

"Meaningful use" will be determined by CMS, but the law states that the EHR must be certified, able to electronically prescribe, part of an electronic exchange and able to report quality measures. Physicians and hospitals will have to demonstrate that they are a meaningful EHR user.

The law also provides incentives from Medicaid for providers who adopt EHR and $2 billion to HHS' Office of the National Coordinator of Health Information Technology to help support health information

exchanges, invest in national HIT infrastructure, provide implementation assistance to providers, and take other actions to advance the use of health information technology.

It is expected that these initiatives will help be the catalyst to move to EHR, according to consultant John Parmigiani, Ellicott City, Md., who helped draft the original HIPAA security rule. "[Government] bodies are working together regarding standardizations. It's a concerted effort to get to e-health care and make it more feasible," he explains.

However, moving to EHRs is still a painful, expensive process, according to attorney Shirley Morrigan, with Foley & Lardner, in Los Angeles. "There is still a lot of patient and provider concern. You need stakeholders' [buy] in. Don't just dump it on people," she says.

The program to encourage EHR use still needs clarification, which is expected in the next few months, says attorney Gerald "Jud" DeLoss with Gray Plant Moody, Minneapolis.

For instance, to qualify for the incentives, the provider must be using a "certified" EHR. However, HIPAA doesn't require EHRs to be certified, and there isn't one standard for certification, although the non-profit Certification Commission for Health Information Technology (CCHIT) currently operates a certification program. So it's unclear if CCHIT's program will become the one required by Medicare to qualify for an incentive, or if other standards will be created, notes attorney Cynthia Stamer, Glast Phillips & Murray, Dallas.

"By 2014, we'll see EHR integrated throughout the country. That's the overriding theme of this legislation," says DeLoss.

Harbinger of more enforcement?

HHS, FTC penalize provider for privacy violations

Check your dumpsters for improperly disposed patient pill bottles, medical records and other sensitive patient information. The federal government is getting serious about HIPAA enforcement.

HHS has signed its second "resolution agreement" regarding HIPAA violations, this time with pharmacy chain and pharmacy benefits manager CVS Caremark, and imposed a $2.25 million fine. But in what many see as a major wake up call for providers, for the first time the FTC also joined in on the action, imposing a settlement agreement of its own on the pharmacy company.

HHS and FTC announced Feb. 18 that the HHS Office of Civil Rights (OCR) and FTC worked jointly to investigate allegations that CVS disposed patient and employee health and other personal information improperly. The agencies found, among other things, that CVS failed to implement adequate policies and procedures to safeguard such information during the disposal process, didn't use reasonable measures to assess compliance with its policies and procedures, and failed to adequately train employees on how to dispose of such information properly.

In addition to the fine, CVS will implement a "robust" corrective action plan and establish and maintain a comprehensive information security program to protect the security of the personal information it collects. CVS also must engage a qualified independent third party to conduct assessments of CVS compliance and render reports to HHS and FTC. The HHS corrective action plan will be in place for three years; the FTC requires monitoring every other year for 20 years.

The enforcement action stems from media reports in various locations that CVS pharmacies threw away pill bottles, employment applications, computer order information and other data containing personal information into unsecured dumpsters. CVS issued a statement Feb. 18 denying that it had engaged in wrongful conduct, that the disposals were "inadvertent," and that it was not aware that any consumer harm resulted.

Why this settlement is significant

This enforcement action is noteworthy not only because of the large size of the fine. It's also the first time that the HHS and FTC collaborated to bring an investigation for a breach of information, and the first time that the FTC has gone after a health care provider for failing to implement reasonable information security practices.

"The FTC/HHS [joint collaboration] is huge. There's going to be an uptick in enforcement on all fronts and more cooperation among agencies," predicts consultant John Parmigiani, Ellicott City, Md., who helped draft the original HIPAA security rule.

But the FTC's involvement should serve as a warning to providers that the stakes just got higher, according to Gerard Nussbaum, director of technology services at Kurt Salmon Associates in New York City. Whereas OCR had taken a more educational approach to enforcing HIPAA (and has been criticized for not taking

more enforcement action), the FTC is "flexing its muscles in its crusade against identity theft," says Nussbaum. In 2008, the agency received more than 313,000 complaints about identity theft, representing 26% all complaints received, a Feb. 26 FTC report says.

"The FTC is a more nasty regulator, and has an entire ALJ [administrative law judge] system, so it's a much more adversarial process. And while OCR is overwhelmed, the FTC has lots of money [to go after violators]," Nussbaum explains.

This case, and the FTC's new authority under the new economic stimulus law to receive notifications of certain vendor HIPAA security breaches *[see related story p. 1]*, indicate that the FTC will become more involved in the protection of personal health information handled by providers, and may lead to turf battles between the two agencies, warns attorney Gerald "Jud" DeLoss, with Gray Plant Moody, Minneapolis.

States add to enforcement effort

The CVS case also is significant because it may signify a trend regarding investigations in how providers dispose of their trash. The Texas attorney general reached a settlement agreement with Select Medical Corp. in July 2008, which had been found dumping patients' personal information in garbage containers. Select Medical agreed to pay the state of Texas $990,000, amend its existing security procedures to ensure future compliance with identity theft prevention laws, post signs detailing records storage and disposal requirements, and implement a new training program. Now that attorneys general have new authority under the economic stimulus law to enforce HIPAA, providers should expect to see more states taking action, says Nussbaum.

"Providers will spend a lot more time defending these things. The FTC likes splashy cases, and [state] attorneys general run for re-election," he points out.

Experts also expect penalties to become more severe. "The educational period is ending. People are supposed to know [about these medical privacy laws] by now," comments Cynthia Stamer, with Glast Phillips & Murray, Dallas.

4 tips to deal with increased enforcement activity

The CVS Caremark settlement (see story, page 4) appears to mark the beginning of stepped up action by HHS and the FTC to protect patient records and identifying information. Consider these preventative actions:

1. **Take your privacy and security obligations seriously.** "If you believe that a breach equals no consequence, you're deluding yourself," says attorney Cynthia Stamer, with Glast Phillips & Murray, Dallas. Make sure you have appropriate policies and procedures to protect patient and employee information, and strong training and compliance programs.
2. **Recognize that your obligation involves more than HIPAA and electronic protected health information (PHI).** HHS investigated CVS for HIPAA violations, but the FTC claimed that the company engaged in unfair and deceptive practices that violated the FTC Act. With the FTC's Red Flag Rules to prevent identity theft set to go into effect May 1 *(see* COR *12/08),* expect the FTC to take more action to stem the identity theft epidemic, says Stamer. "It's not just PHI. It's also financial and other information, and it's paper as well as electronic information," she points out.
3. **Expect more state action.** State attorneys general can now enforce HIPAA as well as use state laws to challenge provider violations. State laws dealing with these issues are growing, says Stamer, so make sure you comply with them as well as federal laws.
4. **Understand the costs involved.** "Be prepared to explain to management why you'll need more money and staff to do your job," says Gerard Nussbaum, director of technology services at Kurt Salmon Associates in New York City. In addition, see if others in your office or facility can help with your compliance efforts.

COs say: Compliance, ethics failures likely to increase

Many compliance officers fear that the decline in the economy will cause an increase in legal and ethics violations. Despite the increase in perceived risk, however, they fear that their budgets to handle noncompliance and do their jobs will be slashed.

This sobering news is from a new national survey by the Health Care Compliance Association (HCCA) and the Society of Corporate Compliance and Ethics (SCCE) conducted in December 2008 and published Jan. 5, 2009. More than 600 compliance and business ethics professionals participated in the survey.

The survey found that 85% felt that the current economy greatly or somewhat increases the risk of compliance and ethics failures. The study also found that 85% expected their budgets would remain stagnant or decline in 2009, and that some staff would be cut.

Fifty-six percent were concerned that their own jobs were at risk. On a slightly brighter note, 49% of respondents reported that senior management saw compliance and ethics as a positive asset, although

FOR THE ANONYMOUS CO:
YOUR QUESTIONS ANSWERED HERE

Q&A

How do I persuade staff to wear their identification badges?

Q Our organization issues identification badges for staff and visitors. I've had several employees who were reluctant to wear their badges and have asked why they have to bother. I know it's important for everyone to wear an identification badge. How do I get that point across to others and get them to comply?

(A version of this question was posed by a medical billing company in Michigan. To raise your own anonymous question, contact Marla Durben Hirsch at 301-299-6155 or at mhirsch@decisionhealth.com).

A There are several reasons why wearing a name badge is important, according to compliance consultant Rebecca Buegel, A*S*K, Avondale, Ariz. Several laws, including HIPAA and the FTC's new red flag rules *(*COR *12/08)*, require organizations to take steps to maintain safety and security of patients, data and the like, so that coworkers, visitors, patients and others know that the employee belongs in the facility or office. If someone isn't wearing a badge, there should be a procedure to stop that person and inquire why a badge wasn't displayed. "If ID badges were not required, imagine how easy it could be for an intruder, dressed as a health care provider or support staff person, to slip into a facility and steal a newborn, steal supplies or access confidential information – no one could easily know if that person belonged or not," she explains.

Organizations accredited by the Joint Commission also must meet the Joint Commission standard that requires the organization to identify staff for security purposes.

The entity's employee handbook should explicitly state that wearing of identification badges is required, and failure to do so could subject the employee to disciplinary action, says Buegel. "If that's not in your policies, you need to update them."

Putting aside the legal requirements, wearing a name badge helps coworkers get to know one another, especially in larger facilities and practices, and gives patients the courtesy and reassurance of knowing who their caregivers are.

However, it can't hurt to ask if there's a particular reason why an employee doesn't want to wear a badge, says Buegel. For instance, if an employee is working with behavioral health patients, she may not want patients to have too much information about her so they can't track down her address or phone number. If that's the case, perhaps it's not necessary for the badge to include the employees' last names.

"But you still need a way for caregivers and patients to know who you are," she adds.

13% believed that management saw it as a hindrance (the remainder saw it as neither).

The study reported that the findings raised several points of concern:

- The perceived increase in the level of risk of legal and ethics failures. "Given the current fragility of the economy, a scandal could be devastating both to the company involved and to the economy as a whole. There is little capacity for the market to absorb bad news," the HCCA/SCCE report stated.
- It is "dismaying" to see that budgetary pressures are being applied to compliance, as the risks can be great and the costs outstrip any near-term savings.
- If a scandal does occur, it would be a mistake to blame the failure of compliance and ethics programs. "The failure may, in fact, be due to a decline in resources for these programs," the study reports.

6 ways to cope

When economy goes down, compliance needs go up

Insiders agreed that 2009 will see more security breaches, incidents of fraud, and other compliance problems. "Breaches will be up because there will be increased pressure to perform and people will cut corners [due to the] pressure," says Roy Snell, CEO for HCCA and SCCE, in Minneapolis. Increasing joblessness will lead to more fraud, hacking and

other compliance problems in health care and other areas, as well, warns Robert Longley, US Government Info, in Citrus Heights, Calif. and a blogger for About.com.

Unfortunately, the compliance department is not a safe haven. "Compliance is a cost center, not revenue generating, so in a recession, you may need to do more with less. It's also such a new area [that management may see it as expendable]," says attorney Cheryl Wagonhurst, Foley & Lardner, Los Angeles.

"In good times people get greedy. In bad times they get desperate," notes Joseph Murphy, author of SCCE's "501 Ideas for your Compliance and Ethics Program," Haddonfield, N.J.

At the same time, we'll also see more regulations affecting compliance and more resources dedicated to government enforcement because of the new administration and Democratic Congress, notes Snell.

"It should be the other way around. Compliance should get more money in this environment," says Wagonhurst.

So what should compliance officers do in these trying times? Consider these steps:

1. **Make sure that you have the support of senior management.** "It's most important that you have authority, even if you don't have money," says Murphy. They need to understand that the organization's "reputation is so important; you can't take any chances with that," says Randall Corley, global compliance officer, Edelman, Chicago.
2. **Work closely with applicable departments.** For instance, work closely with the internal audit department to look for warning signs, such as cash flow not matching reports, suggests Corley. "There will also be more [hot] line activity from former employees or soon-to-be former employers. Some of these tips will be substantive, so make sure that [human resources] is digging down deep enough into this," says Corley.
3. **Delegate some of compliance to other departments.** Other staff can help cover training, audits, site visits and the like if the compliance department can no longer do so. You might want to create a committee of leaders from various departments to help you get the job done, suggests Murphy. "There's no way that one person can implement compliance in a whole organization," Wagonhurst points out.
4. **Work smarter.** "Compliance officers will need to be more efficient and effective. They'll need to stop writing and talking so much and conduct more audits and investigations, focus more on finding and fixing problems, less on policies and procedures," says Snell.
5. **Make sure that access to your systems is cut off as soon as a person leaves his or her job.** "Check that IT is changing passwords and taking other steps," says Corley.
6. **Become a first rate salesperson to sell the importance of compliance.** "Identify with the 'customers' who are the other officers [in your organization] and get them to understand the importance of this subject. Each manager is an individual and thinks a different way. Don't think of 'management' as a block," suggest Murphy. "Keep communication open, promote compliance and create a culture of compliance," adds Corley.

From the Compliance **TOOLBOX**

Code of Ethics for Financial Management – Sample Attestation Form

Here is a sample supplemental attestation for senior management regarding their adherence to a code of ethics, based on language suggested by Randall Corley, global compliance officer, Edelman, an international public relations firm based in Chicago. This form can be used with the sample policy provided in the March 2009 COR. Adopt the form to meet your office's or facility's needs.

1. I will act with honesty and integrity in my professional relationships. I will promote and be an example of ethical behavior as a responsible partner among my peers and subordinates in the work environment.
2. I will avoid conflicts of interest. In doing so, I will ethically handle any actual or apparent conflict of interest in personal and professional relationships and will promptly disclose to [name of your organization] compliance officer the nature of any transaction or relationship that reasonably could be expected to give rise to such a conflict of interest.
3. Any accounting records for which I am responsible will be prepared in accordance with applicable accounting standards and established company practices applied on a consistent basis. Any books, records, and accounts that I am responsible to maintain will be kept in reasonable detail, and will accurately and fairly reflect transactions and dispositions of the company's assets. I will not knowingly falsify any book, record, account or business document.
4. I will comply with applicable laws, rules and regulations of national, regional, provincial and local governments, and other applicable regulatory agencies.
5. I will act in good faith, responsibly, with due care, competence and diligence, and without misstating, misrepresenting or omitting material facts or circumstances or allowing my independent judgment to be subordinated.
6. I will maintain the confidentiality of information acquired in the course of my work, except where disclosure is authorized and appropriate to carry out my assigned responsibilities, or where I am otherwise legally obligated to disclose such information. I will not use confidential information acquired in the course of my work for personal advantage.
7. I will responsibly use and control assets and other resources employed or entrusted to my supervision, including taking appropriate measures to ensure that access to assets or resources is permitted only in accordance with management's general or specific authorization.
8. I will maintain professional skills and share knowledge with my peers and subordinates to enable me to carry out my assigned responsibilities and obligations.
9. I will not improperly or fraudulently influence, coerce, manipulate, or mislead any authorized audit or interfere with any auditor engaged in the performance of an internal or independent audit of the [name of your organization] financial statements or accounting books and records.
10. I will report questionable accounting, internal accounting control, auditing or fraud matters, or allegations of noncompliance with this Code of Ethics for Financial Management to company management. If I do not feel that any such issues raised have been resolved appropriately, I will report my concerns to the [your organization compliance officer, compliance committee or hotline] as provided in the [name of your organization] Code of Ethics and Business Conduct.
11. I will be accountable for my actions and decisions. I acknowledge that failure to adhere to this Code of Ethics for Financial Management or to the [name of your organization] Code of Conduct may result in disciplinary action, up to and including termination, as allowable by applicable local law.

By signing below I acknowledge that I have and will continue to comply with the standards set forth in this Code of Ethics for Financial Management, and that any exceptions have been communicated to the compliance officer and resolved as determined appropriate by the Compliance and Ethics Committee.

Signature; Printed Name; Title; Office; Phone Number