

Strategies for Health Care Compliance

Your guide to effective compliance

Prepare to respond to breaches of privacy

**Practical steps your organization can
take now to avoid federal scrutiny**

While your healthcare organization awaits a breach notification final rule from HHS, there are some practical steps you can take to prepare should you need to notify patients of a privacy breach.

Before an event happens, you should have a plan in place detailing how you will respond to a breach and notify your patients, says **David Behinfar, JD, LLM, CHC, CIPP**, privacy manager at the University of Florida College of Medicine in Jacksonville.

If you need to notify patients of a breach, there are some important elements of the process you should consider, says Behinfar, who spoke at the three-day Fourth HIPAA Summit West meeting in San Francisco October 5, 2010. You won't find these issues in the final rule, he says, since HHS does not formally provide specific guidance on one method of compliance versus another;

rather, it typically leaves covered entities (CE) to work out the details for themselves, he says.

Remember that, upon discovery of a breach of unsecured PHI, the CE must issue notification to affected persons and possibly to HHS and the media.

Take these steps in advance to prepare:

➤ **Plan for computer forensics.** Have a plan in place to address the need for computer forensics, says Behinfar.

If your organization loses possession of an unencrypted laptop computer and you later regain possession of the device, how do you know whether someone accessed the PHI it contained?

The ideal situation is to obtain

"If you ... can internally handle calls on a breach involving 100,000 patients, more power to you."

—David Behinfar,
JD, LLM, CHC, CIPP

results of computer forensics testing before notifying patients of a breach—because you may not need to send notification at all, Behinfar says. The forensics may show that no one actually accessed the information. Your IT personnel may know of a reputable computer forensics lab or person who can perform this service for your organization, he says.

Make sure you know before a breach occurs whom you will call for a forensics examination, Behinfar says.

This is also important because of the time limitations for notifying affected persons, says **John C. Parmigiani, MS, BES**, president of John C. Parmigiani & Associates, LLC, in Ellicott City, MD.

Under the federal breach notification rule, a CE must notify affected individuals as soon as reasonably possible, but no later than 60 days from the time it becomes aware of a breach. However, some states impose a time limit of five days or less for notification, Parmigiani notes.

> continued on p. 2

IN THIS ISSUE

p. 4 Mark down these devices
We list the common devices that should be on your list in terms of ensuring privacy and security compliance.

p. 6 Dealing with RAC denials
This month's idea discusses a step-by-step approach to handle a RAC denial.

p. 8 Management matters
We offer tips and strategies for conducting annual staff evaluations.

p. 10 Let's get social
Check out the details of one facility's social media policy.

HCPPro

Breaches

< continued from p. 1

Research and choose a computer forensic firm, and perhaps have an arrangement with one or more companies that can provide a quick turnaround in the case of a suspected breach, he says.

Being able to determine from a forensic analysis whether PHI was accessed by an unauthorized person is an important first step in establishing whether a breach occurred, Parmigiani says. The notification process—sending letters, setting up a call center, putting out a press release—is time-consuming and expensive, he notes.

Forensics should be unnecessary in most cases if CEs are properly encrypting ePHI, shredding paper PHI, and otherwise following the HHS and National Institute of

Standards and Technology guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, says **Daniel F. Gottlieb, Esq.**, a partner at McDermott Will & Emery, LLP, in Chicago.

You can find HHS' interim final rule on Breach Notification for Unsecured Protected Health Information at <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>.

For guidance that specifies the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, visit www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

However, in certain instances, such as a hacking event, forensics may provide analysis that is helpful to the risk assessment required under the HITECH breach notification regulations or your risk assessments to comply with overlapping state breach notification laws, says Gottlieb.

► **Contract with a call center.** “If you think you can internally handle calls on a breach involving 100,000 patients, more power to you,” Behinfar says. If not, you need to think about contracting with a call center.

As call center services can be expensive, Behinfar recommends that organizations send out a request for proposals and know whom they will use before a privacy breach occurs.

When choosing a call center, know where the center is located—Behinfar advises using a center in the United States. CEs must rely on this company and its employees to handle sensitive information, he says. Companies that are overseas are not subject to U.S. laws and will likely be beyond a CE's reach if they misappropriate any information they are able to access about patients, thus placing organizations in even more trouble.

Several years ago, a call center employee in India misappropriated PHI from a CE and threatened to release it because the call center failed to pay her, Behinfar says. “It was a mess—and the instructive point was that CEs should relay on U.S.-based call centers,” he says.

| Editorial Advisory Board | | Strategies for Health Care Compliance | |
|---|--|---|-----------------------------|
| HCPPro | | Group Publisher: | Lauren McLeod |
| | | Executive Editor: | Ilene MacDonald, CPC |
| | | Senior Managing Editor: | Dom Nicastro |
| <p>Christine Bachrach Chief Compliance Officer Senior Vice President HealthSouth Corporation Birmingham, AL</p> <p>L. Edward Bryant Jr. Partner Gardner, Carton & Douglas Chicago, IL</p> <p>James A. Kopf Former Director of Program Investigation for the OIG President Healthcare Oversight New Canaan, CT</p> <p>Mark L. Mattioli, Esq. Post & Schell, PC Philadelphia, PA</p> <p>F. Lisa Murtha, Esq. Principal Managing Director Huron Consulting Group New York, NY</p> <p>JoAnn Ross, Esq. Attorney Dayton, OH</p> | | <p>Theodore J. Sanford Jr., MD Chief Compliance Officer for Professional Billing University of Michigan Medical Center Ann Arbor, MI</p> <p>William Sarraille, Esq. Sidley, Austin, Brown & Wood Washington, DC</p> <p>Sheryl Vacca Director West Coast Health Care Compliance Practice Deloitte & Touche, LLP Los Angeles, CA</p> <p>Hank Vanderbeek, MPA, CIA, CFE HAV Compliance Services Haverhill, MA</p> <p>Robert A. Wade, Esq. Partner Baker & Daniels, LLP South Bend, IN</p> | |
| <p>Strategies for Health Care Compliance (ISSN: 1542-2844 [print]; 1937-7363 [online]) is published monthly by HCPPro, Inc., 75 Sylvan St., Suite A-101, Danvers, MA 01923. Subscription rate: \$349/year. • Strategies for Health Care Compliance, P.O. Box 3049, Peabody, MA 01961-3049. • Copyright © 2011 HCPPro, Inc. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPPro or the Copyright Clearance Center at 978/750-8400. Please notify us immediately if you have received an unauthorized copy. • <i>Current Procedural Terminology (CPT)</i> is Copyright © 2008 American Medical Association (AMA). All rights reserved. No fee schedules, basic units, relative values, or related listings are included in CPT. The AMA assumes no liability for the data contained herein. Applicable FARS/DFARS restrictions apply to government use. • For editorial comments or questions, call 781/639-1872 or fax 781/639-2982. For renewal or subscription information, call customer service at 800/650-6787, fax 800/639-8511, or e-mail: customerservice@hcppro.com. • Visit our website at www.hcppro.com. • Occasionally, we make our subscriber list available to selected companies/vendors. If you do not wish to be included on this mailing list, please write to the marketing department at the address above. • Opinions expressed are not necessarily those of SHCC. Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions.</p> | | | |

Also consider whether the call center has or offers:

- A performance bond
- Privacy breach experience
- More than one location
- Good references
- The ability to handle calls 24/7, including holidays
- Multilingual staff
- A project manager at management level assigned to handle your breach
- An escalation process to address unsatisfied callers
- Customized reporting
- Detailed pricing
- Training for call center employees on your specific breach
- Assistance with script writing

The CE should require the call center to assign one person to be the lead manager for its specific breach who can work with the CE on daily issues, Behinfar says. You want to speak to the same manager who knows the details of your breach.

A proper escalation process will address disgruntled callers who are unsatisfied with the response they receive. The call center should have a process to transfer an unsatisfied caller to a higher-level management professional who can hopefully satisfy the caller's needs, Behinfar says. The final step in the escalation process is referral to the healthcare organization's privacy officer.

You should line up a call center contractor in advance that you can quickly employ, especially in breach situations affecting a large number of individuals, such as 500 or more, says Parmigiani.

You may be able to handle breaches affecting a smaller number of people in-house, but consider whether your organization can quickly marshal the requisite skills and resources to respond in the limited time requirements, he says.

Gottlieb says that when an organization sends a breach notification letter to a large number of affected individuals, it should engage an experienced call center to handle calls. Call center operators should be trained to respond to anticipated questions.

The organization should require the call center to staff the line with extra operators for the first few days after individuals receive the letters because there will be higher call volume on those days, Gottlieb says.

► **Prepare for printing and mailing the breach notice.** It is not an easy task to print 100,000 letters, says Behinfar.

You need to think about the details of how you would complete a massive mailing. Will you personalize each letter or simply have a "Dear patient" introduction? Who will put together the list of patients and perform the mail merge?

You also need to determine whether your organization will handle the mailing directly or contract out the process in whole or in part, Behinfar says.

If you think you can complete the mailing using in-house resources, ask your mailing center what its capabilities and advance notice requirements are. Can it handle breach notices at the same time that patient statements are scheduled to go out? Once again, you are going to be under tight time constraints to send out the notices.

Tips: Use quality bond paper for the notification letters. Otherwise, your letter may look phony, Behinfar says. Also consider using a mailing service that can check addresses to minimize the amount of returned mail, suggests Gottlieb.

► **Know your plan for creating a press release.** Federal breach notification requirements mandate that CEs notify the HHS secretary and prominent media outlets serving a state or jurisdiction when breaches affect 500 or more individuals.

Make sure you quickly involve your PR department so you can coordinate the timing of mailing the breach notice with the issuing of a press release, Behinfar advises. If you don't have an internal PR department, decide how you will proceed with any media relations, he says.

There are two schools of thought on this issue. The press release is best handled in-house, Parmigiani says,

> *continued on p. 4*

Breaches

< continued from p. 3

either by an organization's PR department or its legal/risk management personnel. Construct your press release in an empathetic way that best communicates with your patients, he says.

"While this could be contracted out, I believe that something may be lost in the delivery of the message," Parmigiani says.

On the other hand, Gottlieb believes the job is best handled by PR professionals who can craft a press release. Unlike other press releases, the goal is not to generate lots of publicity, but rather to demonstrate that your organization is handling the incident carefully, he explains.

► **Be prepared when you file a police report.**

Whether you file a police report depends on the nature of the breach, says Parmigiani. For instance, was physical equipment taken from your organization or was there unlawful entry to your facilities?

If you fill out a police report, be aware that you could be tipping your hand to the media, says Behinfar. So be prepared, as this may force your hand in sending out a press release.

A police report can accelerate the course of events and compel you to complete your breach response plan in a very tight time frame, he says.

Parmigiani agrees a police report can often trigger a media response. You may find your organization in the spotlight for "late-breaking news," and this can force you to hastily prepare and deliver a press release, he says.

Gottlieb says his law firm generally recommends filing a police report.

This demonstrates that the organization is taking the security breach seriously, and it also may be necessary for any insurance claims. If an individual is a victim of identity theft, he or she should also consider filing a police report, he says. ■

Assess the risk to PHI from these devices

The case of a digital camera stolen from an Arkansas hospital highlights the need for healthcare organizations to assess the risk to PHI from a long list of devices.

It's no longer just the traditional sources—things such as laptop and desktop computers, hard drives, and paper records—that healthcare organizations need to worry about. Now organizations must consider just about anything that is electronic that can store data as a potential risk, says **Chris Apgar, CISSP**, president of Apgar & Associates, LLC, in Portland, OR.

Although this list is not meant to be comprehensive, consider the following devices for which a hospital must always account and have a security procedure in place:

► **Digital copy machines.** Newer-model copiers have dual hard drives, says Apgar. Recent news reports have raised awareness of the potential security risk created by these digital copy machines.

Almost every digital copier built since 2002 contains a hard drive, like the ones on computers, that stores an

image of every document copied, scanned, or e-mailed by the machine.

Used copy machines, which are often resold, can contain lots of sensitive information, including PHI.

At the Fourth HIPAA Summit West meeting in San Francisco October 5, 2010, **Adam Greene, JD, MPH**, senior health information and privacy specialist at OCR, asked members of the audience whether they were aware that copy machines can be repositories for PHI and whether they had alerted their staff to the danger.

"It's important that these copy machines don't go out the door with hundreds of records on them," says Greene.

Just as they should when disposing of old computers, healthcare organizations should scrub all the data on copy machine hard drives.

► **Biomedical devices.** This includes common imaging equipment, such as MRIs, CT scans, and EEGs. "They all

maintain patient information," Apgar says. It's not just newer equipment you need to worry about, either. Don't forget about x-ray machines and other biomedical devices that may print PHI. Usually if a machine can print, it has electronic memory, Apgar says.

When these machines become surplus and you are replacing them, you need to wipe the memory clean so that they no longer store PHI.

➤ **Smartphones.** Many of these phones contain a flash card that can plug into a computer. If physicians or other healthcare staff receive e-mail or attachments containing patient information, those data can be stored on the flash card, Apgar says. If the phone is lost or stolen, the PHI stored on it can be breached unless it is encrypted. "And a lot of people don't think about that," he says.

The data may also include photographs.

Also be aware of text messages that healthcare providers might exchange and that are also stored on the phone, Apgar says.

For instance, an anesthesiologist may communicate in the morning with a hospital surgeon about cases that are coming up that day in the operating room. The text messages may include PHI that is then stored in a text message file. Anyone who obtains that phone can access the patient information stored there.

➤ **Netbooks, iPad™ devices, and PDAs.** All of these devices—handheld personal computers—can store PHI and are easily lost or stolen due to their compact size. Such devices are increasingly being used in hospitals and pose a

high risk to PHI, says **Christopher Hourihan**, manager of common security framework development and operations at HITRUST, the Health Information Trust Alliance in Frisco, TX.

Since the devices are essentially mini computers, hospitals can develop applications that provide a portal into their data environment with nothing locally stored, Hourihan says.


"With good authentication to the application, the risk of any data loss is very low," he adds.

➤ **Cellular phones.** Although less sophisticated than smartphones, many regular mobile phones can take and store photographs.

➤ **Office equipment.** This includes fax machines and printers. "They all have memory," says Apgar.

➤ **Camcorders.** Along with digital cameras, healthcare organizations should also think about PHI that may be recorded on video camcorders, Apgar says.

➤ **Digital voice recorders.** Physicians sometimes use these small, compact devices to record their dictation reports, says **Frank Ruelas**, director of compliance and risk management at Maryvale Hospital in Phoenix and principal of HIPAA College in Casa Grande, AZ. But they may not think to delete old reports. Physicians can have reports stored on the device that go back for weeks and that include identifying patient information such as names and medical record numbers. Encourage physicians to erase the dictation reports after storing them on a secure computer, Ruelas says.

| SHCC Subscriber Services Coupon | | | | |
|---|--|--|----------|-------|
| <input type="checkbox"/> Start my subscription to SHCC immediately. | | | | |
| Options | No. of issues | Cost | Shipping | Total |
| <input type="checkbox"/> Print & Electronic 1 yr | 12 issues of each | \$349 (SHCCPE) | \$24.00 | |
| <input type="checkbox"/> Print & Electronic 2 yr | 24 issues of each | \$628 (SHCCPE) | \$48.00 | |
| Order online at www.hcmarketplace.com . Be sure to enter source code N0001 at checkout! | | Sales tax (see tax information below)* | | |
| | | Grand total | | |
| For discount bulk rates, call toll-free at 888/209-6554. | | | | |
|  | *Tax Information Please include applicable sales tax. Electronic subscriptions are exempt. States that tax products and shipping and handling: CA, CO, CT, FL, GA, IL, IN, KY, LA, MA, MD, ME, MI, MN, MO, NC, NJ, NM, NV, NY, OH, OK, PA, RI, SC, TN, TX, VA, VT, WA, WI, WV. State that taxes products only: AZ. Please include \$27.00 for shipping to AK, HI, or PR. | | | |
| | Your source code: N0001 | | | |
| Name _____ Title _____ Organization _____ Address _____ City _____ State _____ ZIP _____ Phone _____ Fax _____ E-mail address (Required for electronic subscriptions) <input type="checkbox"/> Payment enclosed. <input type="checkbox"/> Please bill me. _____ <input type="checkbox"/> Please bill my organization using PO # _____ <input type="checkbox"/> Charge my: <input type="checkbox"/> AmEx <input type="checkbox"/> MasterCard <input type="checkbox"/> VISA <input type="checkbox"/> Discover Signature _____ (Required for authorization) Card # _____ Expires _____ (Your credit card bill will reflect a charge to HCP Pro, the publisher of SHCC.) | | | | |
| Mail to: HCP Pro, P.O. Box 3049, Peabody, MA 01961-3049 Tel: 800/650-6787 Fax: 800/639-8511 E-mail: customerservice@hcpro.com Web: www.hcmarketplace.com | | | | |

This month's idea**Step by step: What to do when you receive a RAC denial**

You receive a RAC demand letter for repayment. But wait a minute before you pay up—you might want to take a close look to make sure your facility was really in the wrong. **Karen Sagen**, managed care leader at Bellin Health System in Green Bay, WI, who has worked in revenue cycle management for the past six years, has developed a step-by-step list of things to consider before pulling out your hospital's checkbook.

"About a year and a half ago I became the RAC coordinator, and I started going to all of the different presentations and webinars and I heard a lot of good ideas," explains Sagen. "So I took notes and put together a checklist of all of the different good ideas that I heard."

Bellin still uses Sagen's checklist; upon receiving each RAC demand, staff members go through it item by item and check each after they complete it. If necessary, they then move on to the second checklist, which guides them through an appeal. Using the appeal checklist helps ensure that they present a thorough picture to the auditor.

"Let's say a patient came in through the ED. That is our key to go back and ask, 'Do we have the ED report? Do we have the ED physician report? What else did they do in the ED? Did they do a CAT scan or MRI? An x-ray? Are all of the tests that they did present?'" Sagen explains. "That way we don't just show what happened when they were admitted to the hospital. Together it builds the big picture for that auditor about what was going on."

One other point to note: Pay close attention to dates, Sagen says. "It's getting worse and worse. The RACs are eating into our time limit. So if you aren't watching those dates, you could really hurt yourself."

This is especially the case if you want to take advantage of the discussion period, which is 15 days. "We had one letter where we had exactly one day left [in the discussion period] when we got it."

That may have been the fault of the post office, but at the end of the day, the only thing you can control is your own process. So have your ducks in a row, Sagen advises. "Know what your process is and be confident in it." ■

RAC denial checklists**Steps to take when a RAC demand for repayment letter is received**

- ❑ Check to see whether the claim has already been audited by another agency.
 - ❑ If the claim has been audited by another agency, notify the RAC auditor by telephone and written documentation.
- ❑ Check to see whether the requested claim falls within the auditable time frame set up by the RAC program or other applicable program.
 - ❑ If the claim is outside the correct audit time frame, notify the RAC auditor by telephone and written documentation.
- ❑ Note timeline for submission of appeal for that particular type of audit/demand for repayment.
 - ❑ Document the time frame on the appeal letter as a reminder of when the appeal must be submitted.
 - ❑ If applicable, update your RAC tracking software.
- ❑ Check to see whether the denial is referencing guidelines from the correct timeline involved. (For example, is the auditor using the local coverage determination retired in 2006 for services rendered in 2009?)
 - ❑ If the wrong local/national coverage determination is being used, notify the auditor by phone and written documentation.
- ❑ Review the credentials of the auditor. Does he or she have the proper credentials for the type of services being audited? (For example, an inpatient auditor does not have the expertise needed to audit an outpatient claim.)
 - ❑ Per the RAC scope of work, providers can request in writing a copy of the auditor's credentials. If you as the provider do not feel the auditor has the correct credentials, notify the RAC by phone and written documentation. Just because the

RAC tells you the auditor is RHIT certified does not mean they are certified in the correct area. You have the right to ask: What is your auditing background? Do you have auditing specialty in the associated area? How many of these types of claims have you audited? What type of provider education can you supply?

- Review the demand letter and clinical information with case management (CM). Does CM feel there is a good chance to have a discussion with the RAC auditor prior to filing a written appeal?
 - If so, call the RAC auditor to set up an appointment for discussion of the account.
- If the demand letter is for an inpatient claim, are there proper orders and documentation to support the inpatient stay?
 - Highlight each area or record and reference in your appeal letter the highlighted areas, along with any clinical information, guidelines, rules, etc., that pertain to the denial.
- Is the discharge disposition correct?
 - If not, follow hospital protocol to correct it.
- If all is in order and your facility is going to appeal, follow the Medicare/RAC appeals checklist below.

Medicare/RAC appeals checklist

Note: The following items should be included every time a Medicare/RAC appeal is done. Each of these items will help create a clearer picture and will allow for a more efficient process. Any time you can stop a question before it is asked, you will be ahead of the game.

- Medicare appeal form (must be the correct form for the level of appeal you are submitting)
- Medical records, including:
 - Face sheet
 - Coding summary
 - Labs
 - Nursing notes
 - Pharmacy records
 - History and physical documentation
 - Physical, occupational, or speech therapy notes, when applicable
 - Progress notes
 - Operative/procedure reports
 - Radiology, when applicable
 - Consult reports
 - ED report, when applicable
 - Physician orders (check status, must be signed and dated)
 - Start and stop times, when applicable
 - Discharge planning/summary
- Local and national coverage determination
- Medical necessity documentation
- Copy of guidelines used to make medical or coding determination
- Documentation of the rationale for the coding, using ICD-9-CM coding conventions, *ICD-9-CM Official Guidelines for Coding and Reporting*, and AHA's *Coding Clinic* information, if available
- Copy of facility signature log for attending physician (if no signature log is available, have an attestation agreement signed and include this with the appeal)

Source: Karen Sagen, managed care leader at Bellin Health System in Green Bay, WI. Reprinted with permission.

Management matters

Strategies for performing staff evaluations

Five things to keep in mind when conducting your reviews

With the end of the year approaching, you, along with many of your HIM director and manager colleagues, may soon be tasked with conducting annual staff evaluations. Chances are it isn't your favorite task of the year. But it needs to be done.

"It's a great idea to have [evaluations], but it is really hard to do it well and make it meaningful. And you certainly don't want to use it to discourage anybody. That's the total opposite of what you want to be doing," says **Chris Simons, RHIA**, director of utilization management and HIMS and privacy officer at Spring Harbor Hospital in Westbrook, ME.

So how can you make evaluations positive and meaningful for your staff and maybe learn something yourself in the process? Simons, along with **Glennnda Gore, RHIA**, vice president of risk management and quality services and chief compliance officer at McAlester (OK) Regional Health Center, **Jean S. Clark, RHIA, CSHA**, director of accreditation at Roper Saint Francis Healthcare in Charleston, SC, and **Monica Pappas, RHIA**, president of MPA Consulting, Inc., in Long Beach, CA, provide strategies for directors, managers, and supervisors facing the daunting task of staff reviews.

Communicate like crazy

One point on which our experts wholeheartedly agreed: Staff members should never be surprised by their evaluations. "There should have been feedback along the way," says Gore. "If an employee's productivity is down throughout the year, they should not hear about it for the first time during their annual evaluation."

Clark suggests managers review productivity and quality monthly for each employee. If employees aren't meeting standards, managers should meet with them to look at their goals at least quarterly. They can then create an action plan to bring performance up the next quarter. She also suggests sitting down with employees every

six months to review goals and identify opportunities for improvement. "The goal should be to keep communication going throughout the year and correct any issues before the evaluations come up," Clark says.

Constant communication will make annual reviews easier, and it can also encourage employees. "I think that we forget how important [feedback] is to an employee. Most people want to know how they are doing," Pappas explains. Even if you are obligated to provide feedback once per year, consider making it more frequent.

Plan ahead

Some facilities conduct reviews annually based on an employee's date of hire. Others pick a single day of the year by which managers must review every staff member. Planning is crucial, especially for those who have to conduct reviews for 10, 20, 30, or even 40 staff members at a time. But regardless of your facility's approach, be thinking about reviews "from the beginning of the year, all year long," says Clark.

Gore suggests keeping files for employees that can be added to throughout the year. Doing so helps remind her of everything that happened during the year when evaluation time comes around. Remember to tuck away both negative items (e.g., formal and informal counseling) and positive items (e.g., quality or productivity reports, compliments received, instances of outstanding work).

Accentuate the positive

Annual reviews shouldn't feel like a trip to the principal's office, says Pappas. "Managers really owe it to employees to figure out good communication strategies throughout the year so there are no surprises," she says. If the only time an employee has this type of exchange with a manager is on an annual basis, nerves are likely to be on edge. However, if a manager and an

employee communicate effectively on a regular basis, employees are less likely to be anxious about what they will hear, she says. But how can you keep reviews positive?

Use the review as a time to set goals, says Pappas, who believes goal-setting should be a mandatory component of employee evaluations. Don't limit goals to increased productivity or quality—employees might want to set goals that will help them advance their careers, such as completing a course or gaining a credential.

You can also use the review as a time to encourage employee ownership of their work. It might start with allowing employees to contribute to their evaluations, suggests Clark. If someone gives them a note or e-mail about an exceptional job they've done, allow them to add it.

Simons agrees that allowing employees to take ownership of their performance is key.

"It's the difference between renting and owning. If you rent a house, you don't take good care of it the way you do when you own it. So you can apply that concept to your work," she says. "People who own their work really care about it." Conducting meaningful reviews is one way to increase ownership—always a good thing.

Simons says it is also important to make the review a learning experience and use it to diminish the distance between you and your staff members.

Another point to address might be an employee's contribution to the big picture, says Pappas. Employees may not understand why their jobs are important, and reaffirming their worth is a nice pat on the back. "HIM is kind of an assembly line, and we have a lot of people who do one step of the process and they really forget or don't understand how valuable they are," she says. "Having them understand the big role of HIM in the EHR and in revenue cycle makes them feel good about what they do."

Keep reviews objective and consistent

Say goodbye to subjective reviews and move to objective, measurable goals, experts say. For example, a goal

might be to attend three continuing education courses on ICD-10 implementation within the next year, or to improve customer satisfaction scores in the area of "overall friendliness" by 15% over last year's score, suggests Gore. Without measurable goals and supporting documentation, it is hard to be objective—which is absolutely critical for evaluations.

Speaking of goals, Clark's facility not only sets targets, but also stretches goals based on productivity and quality, giving employees something to reach for.

Another problem some larger departments may face is inconsistency between reviewers. "If you have a large department and you have a director and a couple of managers and several supervisors, and you've got three to five or 10 people evaluating employees, you have to do something to ensure there is some level of consistency," Clark explains. "You need to be sure that all supervisors within a department are evaluating the same way or you really are asking for trouble."

Bridge the gaps

Your staff member feels she met productivity standards. You, however, are quite sure she did not. Now what? First of all, having objective measures is critical for when these types of situations arise. You never want to say, "This is my opinion," says Clark. You need concrete, measurable evidence, which you can use when sitting down and discussing matters with the staff member.

If done with respect, such a discussion can be quite meaningful, says Simons.

Managers should also be sure to examine the cause of the discrepancy. "Are you way off the mark? Is the employee? Do they not understand what your expectations are? There's clearly an opportunity to see why there is such a big difference between your perception and theirs and try to bridge that," Simons says.

Pappas agrees that huge discrepancies are a sign that there's been a communication breakdown. "And I think that's a big part of what management is: being sure that employees understand the goals," she says. ■

Sample policy**The Vanderbilt University Medical Center's social media policy**

Editor's note: Consider adapting these policy and procedure guidelines to fit your organization's needs.

Social media policy and guidelines**I. Outcome goal**

To provide guidelines outlining how Vanderbilt University Medical Center (VUMC) supports institutional communication goals.

II. Policy

VUMC offers support of institutional communication goals and provides social computing guidelines for VUMC faculty, staff, and students engaging in online discourse and identifying themselves with VUMC.

This policy is not intended for Internet activities that do not associate or identify a faculty or staff member with VUMC, do not use Vanderbilt e-mail addresses, do not discuss VUMC, and are purely about personal matters.

III. Definitions

Content owners, for the purpose of this policy, are those assigned the responsibility of maintaining, monitoring, and moderating a VUMC social media platform. Official communications refer to those done in VUMC's name (e.g., a Vanderbilt Heart Facebook page).

- a. Content owner:** Assigned by department as the individual responsible for monitoring and maintaining Web content.
- b. Moderator:** Assigned by content owner and/or department as the individual responsible for moderating comments and postings by internal and external users, including deleting comments and postings that do not meet the criteria set forth in this policy.
- c. Social media platforms:** Technology tools and online spaces for integrating and sharing user-generated content in order to engage constituencies in conversations and allow them to participate in content and community creation. Examples are Facebook, Twitter, LinkedIn, and YouTube.

IV. Specific information**a. Official institutional Web 2.0 communications**

1. Because of the emerging nature of social media platforms, these guidelines do not attempt to name every current and emerging platform. Rather, they apply to those cited and any other online platform available and emerging including social networking sites and sites with user-generated content. Examples include but are not limited to:
 - a. YouTube
 - b. Facebook
 - c. iTunes
 - d. LinkedIn
 - e. Twitter
 - f. Blogs
 - g. Social media content that is hosted internally and protected by VUNet ID/password

Source: Vanderbilt University Medical Center. Reprinted with permission. For the full form, go to <http://tinyurl.com/28zq82t>.

Strategies for Health Care Compliance 2010 index

EHR

Federal regulations emphasize encryption, risk assessments. April, p. 9.

Financial incentives may fuel meaningful use of EHR. April, p. 11.

HHS addresses privacy, security concerns in EHR program. Sept., p. 10.

Make sure your EHR measures up: Meet meaningful use standards to qualify for Medicare incentives. Nov., p. 11.

Meaningful use checklist for hospitals. Nov., p. 11.

Proposed EHR certifying program seeks to balance needs. June, p. 11.

HIPAA

Back to the drawing board: As attention shifts to HITECH, don't forget about compliance with HIPAA basics. Oct., p. 1.

Beware: Laptop computers create a major security risk. Aug., p. 5.

Develop effective strategies for your breach notification response program. Jan., p. 6.

Five stumbling blocks hinder HIPAA compliance. March, p. 12.

Four steps you must take if a laptop computer is lost or stolen. Aug., p. 7.

HHS breach notification form. Jan., p. 8.

HIPAA Q&A: Business associate requirements, audit log retention periods, and health plans. March, p. 4.

HIPAA Q&A: Compliance with cameras in rooms; requesting donor information; access to records and legalities. Nov., p. 8.

HIPAA Q&A: NPPs, BA contracts, Red Flags Rule, and more. Feb., p. 12.

HIPAA Q&A: Terminate contract if vendor denies records request; patient also can be liable for lost records. April, p. 12.

HIPAA refresher: Handle potential privacy breaches. June, p. 12.

Learn from other healthcare organizations' compliance mistakes: Review the top breaches of 2009 and how you can prevent the same at your facility. March, p. 1.

Managing business associates. March, p. 11.

Red Flags Rule: Consider amending your BA agreements. Oct., p. 4.

Red Flags Rule: Prepare for FTC's June enforcement date. Feb., p. 1.

Reduce your risks by training your workforce. Dec., p. 6.

Responding to identity theft a three-step process. Feb., p. 3.

Sample Red Flags letter. May, p. 5.

Sample Red Flags Rule language? Nov., p. 6.

Seven steps to comply with the Federal Trade Commission's Red Flags Rule: Prepare now. May, p. 1.

The steps one hospital takes to prevent breaches. March, p. 3.

Strengthen your security evaluation process with these five tips. Sept., p. 8.

10 tips for training your workforce to be HIPAA ready. Dec., p. 4.

Update your policies and procedures now; create timelines for checkpoints. Dec., p. 1.

Use this checklist to help evaluate your organization: How does your information security program stack up? Sept., p. 6.

What you need to know about the Red Flags Rule. May, p. 3.

When is it a PHI breach vs. an internal incident? Nov., p. 6.

Medical records/HIM

HIM central to surviving recovery audit contractors as auditing activity is on the rise. July, p. 10.

Medical record documentation makes Joint Commission top 10 noncompliance list for first half of 2010. Dec., p. 7.

Who needs what now? Make sense of the multitude of auditor requests for medical record documentation. April, p. 4.

> *continued on p. 12*

2010 index

< continued from p. 11

Medicare compliance

Brush up on sequencing as RAC complex reviews

get under way in your organization's region.

April, p. 7.

California-based IRFs reflect on their experiences during

RAC demonstration project. April, p. 1.

CMS proceeds with documentation 2.9% payment cut

in FY 2011 IPPS final rule: Coding practices believed to not reflect actual increases in patient severity.

Oct., p. 9.

Comply with CMS guidelines for cardiac, pulmonary

rehab. May, p. 5.

Dig deep into PEPPER even when data look good.

July, p. 3.

Distinguish between ABNs for covered, noncovered

Medicare services. June, p. 5.

Eliminate missed charges, errors to reduce lost revenue.

Jan., p. 1.

Establish a robust coding audit program. July, p. 4.

Five tips to ensure HAC, POA, and never event

compliance. Dec., p. 9.

Identify and audit top Medicaid enforcement targets.

Feb., p. 10.

Know when to report uncertain diagnoses.

March, p. 6.

Lessons learned from MGH's Joint Commission laboratory survey: Perform mock tracers, know the updated

format. June, p. 8.

Master modifiers to ensure accurate reimbursement.

Jan., p. 4.

OIG includes readmissions, inpatient psych in *Work Plan*.

Feb., p. 7.

Prevent and react to outpatient never events.

March, p. 8.

Sample internal audit calendar. July, p. 5.

Seven tips to keep your coding compliance program

fresh. May, p. 8.

Should you provide a voluntary ABN? June, p. 6.

Take advantage of nine tips for RAC appeal success.

Oct., p. 6.

Use PEPPER to improve coding compliance. July, p. 1.

Why you may lose money because of medical necessity.

May, p. 9.

Guide to HIPAA Auditing, Second Edition

Practical tools for privacy and security compliance

This new edition of a best-selling book delivers the hands-on tools and guidance you need to conduct effective in-house audits and stay off the government's radar. *Guide to HIPAA Auditing, Second Edition*, by noted HIPAA expert **Margret Amatayakul, RHIA, CHPS, FHIMSS**, is your blueprint for success. She uses practical examples from real-life situations to demonstrate how you can lower risk exposure.

The guide delivers a comprehensive combination of up-to-date information and tools to facilitate HIPAA audit preparation and risk prevention.

Ask your customer service representative about money-saving discounts and bulk orders. Call toll-free 800/650-6787 or e-mail customerservice@hcpro.com.

Miscellaneous

Compliance officers highly educated, but not rewarded for 'stressful' position. Aug., p. 1.

Medical entry review. Sept., p. 4.

Medical error disclosure program found to reduce lawsuits. Oct., p. 12.

New CDI practice brief offers guidance, focuses on establishing compliant CDI programs. Sept., p. 5.

Physician report card. Sept., p. 3.

Report card helps track timing and dating success. Sept., p. 1.

Stay out of court with effective communication: Avoid mammography lawsuits with these tips from our industry expert. Aug., p. 9.

Use these cost-effective ways to ensure compliance. June, p. 1. ■