

Electronic HEALTH RECORDS BRIEFING

Your guide to transitioning from a hybrid to a paperless environment

Medical identity theft raises new questions for EHRs

In the electronic world, medical identity theft—including theft involving insurance information—is a game-changing phenomenon.

Not only does this type of theft rob patients of their identity, it also compromises the integrity of medical records, either through fraudulent claim submission or fraudulent insurance use. Thieves can change blood type, prescription, disease history, and psychological history information.

Medical identity theft is an information crime that can bring physical—even-life threatening—harm to its victim. With the boost in information-sharing, this healthcare-related crime is drawing plenty of attention from the American public and mainstream media. In fact, the media and watchdog groups are already asking new questions.

As healthcare information crimes become more

prevalent, experts are leveling criticisms against EHRs and RHIOs. The argument is that modern digitized healthcare environments create patient information rapidly within healthcare provider organizations and between regional providers.

If an information crime compromises the integrity of medical records, then the fraudulent information propagates quickly, and probably irreparably, through the records.

This leads to the question that has the industry buzzing: Are EHRs more vulnerable than traditional systems?

The answer is “not necessarily.” If hospitals take the proper steps to protect the safety of their patients—through appropriate auditing and security safeguards—the digitization of healthcare provides greater security and safety for patients. However, without new security and auditing safeguards, hospitals are putting their patients at risk.

Coming next month:

Columnist Darice Grzybowski shares the top 10 pitfalls to avoid during EHR implementation.

Power comes with responsibility


Healthcare information systems and EHRs provide remarkable efficiency and quality of care benefits relative to patient care. However, a rogue hospital insider can use that same digital leverage to commit information crimes against patients and your institution.


The catch is that hospitals must provide relatively broad electronic access to patient records because so many personnel collaborate to deliver the best care possible. Also, employee access to health information systems is broad, because if a patient dies because hospital personnel could not access the right information, the


> continued on p. 2





IN THIS ISSUE

p. 3  **Identity theft statistics**
Only half of consumers feel that their healthcare providers are effective in protecting their medical records.

p. 5  **Information security**
A hospital in Atlanta confirms that the OIG audited the facility and that it looked at technical aspects of HIPAA's security rule.

p. 6  **Stuck implementations**
Some EHRs don't work. Here's how to make sure that yours does, and what to do in case your project hits a snag.

p. 8  **Training**
How one healthcare system trained 11,000 staff members in less than a year.

p. 12  **Tech Talk**
You might be surprised at how large and vocal the EHR blogging community is.

Identity theft

< continued from p. 1

ramifications are enormous. The collaborative nature of healthcare information systems makes them enormously vulnerable to a wide variety of privacy breaches by criminal or unethical insiders.

Educate staffers on scenarios and risks

Because the electronic healthcare environment lends itself to privacy breaches, it is important to educate your staff on the scenarios and why there is institutional risk.

Some breaches may seem harmless but are frequently tied to highly risky legal scenarios in which healthcare providers find themselves in the middle of divorce, child custody, blackmail, identity theft, and organized crime court cases.

At the extreme end of risks is medical identity theft,

in which patients suffer financial, professional, emotional, and even life-threatening consequences. Consider the following broad set of electronic breaches:

- ▶ Medical identity theft. This information crime almost always involves a hospital insider in collusion with organized crime. For a good example of this type of crime, consider the Department of Justice's recent prosecution of Fernando Ferrer Jr., who paid a hospital insider at Cleveland Clinic for information about 1,130 patients. Ferrer then used the information to wrack up \$7 million in Medicare claims, for which Medicare paid \$2.5 million. As of presstime, Ferrer is awaiting sentencing, scheduled for April 27. Unfortunately, the patient victims will be working to clear their medical records for years to come.
- ▶ Identity theft. Hospitals possess much of the same information as financial institutions, so it shouldn't come as a surprise that thieves are stealing and selling patients' Social Security numbers, names, and dates of birth, often to organized crime. The hospital insider can be anyone, including physicians, nurses, and administrative staff members. Usually, the insider is an administrative, help-desk, or services employee who feels that he or she is underpaid and undervalued. And selling patient information can be lucrative for him or her.
- ▶ Family member snooping. These incidents are most closely tied to divorce and child custody cases. Often, an estranged spouse who is a hospital employee uses confidential medical records to gain an upper hand during financial or child custody negotiations.
- ▶ Neighbor snooping. Neighbor snooping can have several motivations, but is often involved in blackmail cases. Common neighbor snooping incidents involve an unauthorized hospital employee examining highly sensitive information, such as psychiatric records. This can result in a highly litigious situation if the victim believes that a hospital's information system and employee are involved.

Editorial Advisory Board *Electronic Health Records Briefing*



Group Publisher: **Lauren McLeod, CPC-A**
 Executive Editor: **Ilene MacDonald, CPC-A**
 Managing Editor: **Andrea Dickey, CPC-A**, adickey@hcpro.com,
 781/639-1872, Ext. 3856

Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

President
 Margret\A Consulting
 Schaumburg, IL

Jill Burrington-Brown, MS, RHIA

Practice Manager
 American Health Information
 Management Association
 Chicago, IL

John R. Christiansen, JD

Attorney at Law
 Christiansen IT Law
 Seattle, WA

Michael Glickman

President
 Computer Network Architects, Inc.
 Rockville, MD

Darice M. Grzybowski, MA, RHIA, FAHIMA

President
 HIMentors, LLC
 La Grange Park, IL

Lynne Henderson, MHA, RHIA

Corporate Director of Health Informatics
 Spartanburg Regional
 Healthcare System
 Spartanburg, SC

Kelly McLendon, RHIA

President
 Information Management
 Titusville, FL

Rod Piechowski

Vice President, Technology Leadership
 The National Alliance for Health
 Information Technology
 Chicago, IL

Cheryl Servais, MPH, RHIA

Vice President, Compliance & Privacy Officer
 Precyse Solutions, LLC
 Wayne, PA

Claudia Tessier, CAE, RHIA

Vice President
 Medical Records Institute
 Boston, MA

Electronic Health Records Briefing (ISSN 1554-3293) is published monthly by HCPro, Inc., 200 Hood Lane, Marblehead, MA 01945. Subscription rate: \$279 per year. • Send address changes to **Electronic Health Records Briefing**, P.O. Box 1168, Marblehead, MA 01945 • Copyright 2007 HCPro, 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 HCPro, Inc., or the Copyright Clearance Center at 978/750-8400. • 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@hcpro.com. • Visit our Web site at www.hcpro.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 EHRB. 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. **Electronic Health Records Briefing** is not affiliated in any way with The Joint Commission.

► Very important patient (VIP) snooping. VIP medical record snooping is nearly impossible to stop without proper auditing safeguards and education. There is a well-documented case involving former baseball player Darryl Strawberry. He checked into a New York hospital, and employees examined his record 365 times. An internal audit discovered that, at most, only 3% percent of the record access was related to his care. It is now routine practice to

dismiss employees who violate patient privacy in this manner. Hospital executives who receive care at their own hospital are well aware of the risks of curious or disgruntled employees viewing their medical records. In rural, close-knit communities, where healthcare options are limited, this scenario plays out time and time again—often to the embarrassment of the healthcare provider.

> *continued on p. 4*

ID theft by the numbers

Editor's note: EpicTide in St. Petersburg, FL, partnered with The Benchmarking Company and New London Consulting in November 2006, to conduct this survey; prepare the results. About 501 people completed the survey, and participants working in the healthcare industry or in a research firm opted out of completing the survey.

Four percent of survey respondents reported that they have been victims of medical identity theft.

Eighteen percent of the victims of medical identity theft reported that a family member was responsible for the theft.

Respondents' top three concerns were:

- 1.** Potential risk to their life/health (**58%** report this as one of their top two concerns)
- 2.** Loss of privacy and confidentiality of their medical records (**35%** report this as one of their top two concerns)
- 3.** Changes to their medical records as a result of medical identity theft (**59%** report this as one of their top three concerns)

HIPAA

Only **53%** of respondents reported being asked to sign an acknowledgement of receipt of a notice of privacy practices at a physician's office, hospital, pharmacy, or medical organization.

One in every two respondents reported that they have not read the notice of privacy practices at a physician's office, hospital, pharmacy, or medical organization.

Of the respondents who read the privacy notice, **88%** stated that they understood their patient rights. However, when asked specific true-or-false questions about their rights, **35%** of responses were incorrect.

Access

Forty-three percent of survey respondents said they believe it is legal for healthcare employees to look at their medical records without written consent or knowledge.

One in every two consumers said they believe that their healthcare provider does not know when someone accesses their medical records.

Less than **half (40%)** of consumers said they feel confident that their healthcare providers are able to secure their medical records and personal information.

Only **half** of consumers reported that they feel their healthcare providers are effective in protecting their medical records.

Breaches

Ninety-eight percent of survey respondents said they believe healthcare providers have a responsibility to inform patients if they suspect an unauthorized person has accessed or compromised patient records.

Seventy-eight percent of survey respondents said they feel healthcare providers should inform patients of a possible security breach within 24 hours. One hundred percent of respondents believe providers should inform patients within one week of the suspected breach.

Source: EpicTide, Inc.

Identity theft

< continued from p. 3

► Criminals and the accused. Like VIP snooping, this category involves well-known people who check into hospitals. However, in this case, they are locally or nationally infamous. Hospital employees frequently access medical records outside the scope of their job, learning compromising information related to law enforcement investigation and prosecution. Not only do these staffers compromise the patient's legal rights, they and the hospital can find themselves in the middle of criminal prosecution. Law enforcement may also coerce hospital workers to disclose information about patients so that they can complete an arrest.

Proactively address emerging privacy and security challenges

Electronic privacy auditing systems rely on clues related to specific uses or scenarios. Examples of these clues include an employee reviewing an entire family's medical records (snooping and medical identity theft), printing out unusual volumes of patient records (identity theft and medical identity theft), or frequently changing patient contact information, such as phone numbers and addresses (medical identity theft).

Leading healthcare providers committed to a digital environment are using electronic privacy auditing to safeguard their medical records and protect their patients. They are using electronic privacy auditing to do the following:

- Automate complaint-driven patient privacy audits
- Automate tip-driven employee/user audits
- Replace random, manual patient audits with comprehensive electronic audits to identify tell-tale signs of privacy violations
- Reinforce HIPAA and security education with electronic auditing, which automatically audits and detects high-risk scenarios
- Establish a ticket-management system that delegates and tracks the resolution of a potential privacy breach to a manager of the department involved in the incident

📊 Prepare for support through a court trial

Train, train, train

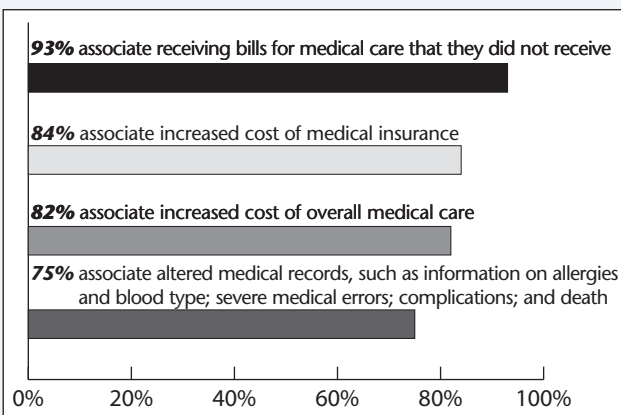
Your hospital's privacy and information security officers should regularly conduct educational sessions on scenarios that the staff should watch for; the potential personal, financial, professional, and health consequences to the patient; and the institutional risk to the hospital. Remember, education doesn't succeed without the ability to catch and reprimand the offending insider who takes advantage of his or her medical record access privileges. This is where electronic privacy auditing plays a major role. Staff education really takes hold when you put in place electronic systems to detect any inappropriate access.

Electronic privacy auditing can be entirely thorough, whereas a random audit of 25 paper patient records per month has little effectiveness in detecting information crimes. ■

Editor's note: Kurt Long, CEO of St. Petersburg, FL-based privacy auditing company EpicTide wrote this article. For more information, go to www.worldprivacyforum.org and click on the medical identity theft link.

Consumer-identified consequences of medical identity theft

The number of survey respondents who associate the following as possible consequences of medical identity theft:



Source: EpicTide, St. Petersburg, FL. Reprinted with permission.

OIG audits focus on security; watch your EHRs

The Office of Inspector General (OIG) says it is in the process of conducting HIPAA audits of covered entities. A hospital in Atlanta confirms that the OIG audited the facility and that it looked at technical aspects of the security rule.

This isn't surprising, says Reece Hirsch, Esq., partner at Sonnenschein Nath & Rosenthal, LLP, in San Francisco. "From a political standpoint, there's been a perception that [HHS] has been less rigorous than it might have been in enforcing all aspects of HIPAA," he adds.

Expect renewed enforcement

A source at the OIG says that the 2007 *Work Plan* addresses the possibility of HIPAA audits in a section dealing with HIT. "The wider use of [EMRs] and [PHRs] raises concerns over privacy and security of patient data," the agency said on p. 58 of the document.

In addition to practical HIT concerns, the government may just be embarrassed, Hirsch says. "This may be driven in part by the high profile of many security breach incidents," he says. The OIG's security audits come on the heels of a series of security breaches both in and out of the healthcare industry, including several at the Department of Veterans Affairs.

A December 2006 security guidance from CMS regarding the use of mobile devices and storage media was also a signal that CMS is focusing new attention on security rule compliance, Hirsch says. (Go to www.cms.hhs.gov/securitystandard and scroll down to the "Downloads" section to access the agency's remote security document.)

"If you look at the history of CMS and the Office for Civil Rights [OCR] with HIPAA enforcement, they try to be good guys," says **John C. Parmigiani**, president of John C. Parmigiani and Associates, LLC, in Ellicott City, MD, and former director of enterprise standards for the Health Care Financing Administration (now CMS).

Parmigiani was also chair of the governmentwide HIPAA administrative simplification security and

electronic signature standards implementation team. CMS and OCR have largely depended on voluntary compliance to ensure HIPAA's effectiveness. On the other hand, he says, "the OIG never has a problem being the bad guy."

Dust off your risk analysis

Whatever the OIG's motivation, the audits mean that HIPAA security should be a priority for covered entities—especially those that have only paid lip service to the security rule since its April 2005 compliance date.

Many covered entities still have not performed a comprehensive risk analysis, says **Kevin Beaver, CISSP**, an independent consultant with Principle Logic, LLC, in Acworth, GA. If you haven't done this or have conducted little more than a checklist audit since then, now's the time to act, because the risk analysis is a natural starting point for an OIG review, he adds.

"The OIG likely isn't going to have all these fancy vulnerability assessment tools or the technical security analysts that can go in and find a lot of the technical vulnerabilities," Beaver says. "Instead, they're likely going to have higher level auditors that are looking at higher level things." This means that having an updated risk analysis—documentation to support any variances between addressable requirements under HIPAA and what your facility implemented—and being able to show security-related policies and procedures are especially important. It will also help to show that you understand your vulnerabilities from a technical perspective.

Beaver suggests information security officers take the following steps to prepare for possible OIG auditing:

1. Refamiliarize yourself with the security rule.
2. Revisit your facility's risk analysis, making sure that it remains valid through any changes in your environment. A risk analysis that is more than a year old is likely too stale.
3. Don't spend so much effort on operational security

> *continued on p. 10*



Revive a stalled implementation project with 'quick wins'

Editor's note: This article is the second in a two-part series.

If you're already in the middle of your implementation but haven't done the proper prep work, you should go back and take care of the details now. Last month, **EHRB** explained why some projects don't work—cultural resistance to change and failure to do the “hard work” up front.

Do a proper prep

“The secret to success is thorough preparation,” said Susan Ordway, senior director of HIT services and manager of the Doctors Office Quality Information Technology (DOQ-IT) program for quality-improvement organization (QIO) Masspro in Waltham, MA. Ordway spoke during the February Healthcare Information and Management Systems Society conference in New Orleans. For the first two steps you must take to prepare, refer to the April **EHRB**. Then, after you've conducted an assessment and drafted a plan, take the following steps:

► Step three: Select a vendor

By this step, your organization should be “change-ready,” which means it is now in a good position to decide on a vendor that fits well with its plan. This isn't a decision to take lightly. “This system will become the center of your universe,” said Ordway.

Think back to the case-study in part one of this article: An independent practice association (IPA) with 400 physicians and 50 practices, located across two counties, decided to select and implement an EHR with a pilot of four practices, and then roll it out to all of its practices within three years. The physicians working with the IPA's CIO led the effort and decided to “take the path of least resistance and select the EHR from their practice management vendor, in order to start the project quickly,” said **Charles Parker**, vice president and chief technology officer at Masspro, the QIO that consulted on the pilot, and also a speaker during the February conference. The prac-

tice management vendor had just released its certified EHR, and the IPA assigned the physicians resources and hired a project manager to make the pilots happen.

Did you catch their mistake? They took the path of least resistance and selected a product from their practice management vendor so they could start the project as soon as possible. “It's a very bad decision to take the easy route,” said Ordway. Because the IPA made a hasty decision, one physician completely refused to use any part of the system, which made one office operate in a dual-workflow environment. Dual workflow is hardly the desired result of an EHR.

“What you need to do is select a long-term partner, not a product,” said Ordway. The vendor should have the following:

- Vision and culture. You want to find a partner that has a similar vision and culture to your organization. When you both are working toward the same goal, you'll be more likely to have success.
- Services. A product isn't great without the support to back it up. Having a vendor that can troubleshoot and support you every step of the way is crucial.
- A solid product. Even with great support, if the vendor doesn't have the technology, your organization won't be able to operate the way it should.

► Step four: Redesign your organization

EHR implementation is the best time to improve operational efficiency at your organization, because the reason you are going electronic is to be a better place to give and receive care. This means you don't want to take a bad paper process and convert it to an equally bad electronic process. It defeats the purpose of EHRs.

“You should harness the opportunities of electronic information,” said Ordway. Use EHR implementation to redefine your processes, procedures, and workflows.

Paper is fundamentally different and relies on triggers that won't work when you're using an EHR. For example, in the

paper world, you might place a patient's chart in a bin to indicate that the patient has arrived and is ready to see a physician. This won't work with an EHR. You'll need to consider an electronic trigger that works the same way. It can be a challenge to think of all of the possible workflow changes you'll have to make. Consider re-designing the following main areas:

- ▶ Patient flow
- ▶ Point-of-care documentation
- ▶ In-office communication
- ▶ Document management
- ▶ Chart abstraction (migrating away from this process)

If this seems overwhelming, make a list of every detail of your current process. For example:

1. Patient needs a medication refill
2. Patient calls refill hotline
3. Nurse manning the hotline documents and deletes the messages
4. Nurse manning the hotline prioritizes the messages
5. Nurse manning the refill line creates a list of charts to pull and delivers the list to the HIM department

Alternately, you can also make flowcharts that show workflow in the paper environment. In many cases, you'll learn something new about your facility. For example, you may say to the scanning manager, "I never knew you did that," or, "Why is [staff member] the only person able to do this?" This organization will help you cover all of your bases. Once you've made lists or flowcharts, redesign the most efficient processes possible for your EHR. Minimize the number of people and steps in each process.

This becomes your "future state," said Ordway. It will be the basis for how you set up your EHR during implementation. In the end, "you don't want a foot in each camp," Ordway said. "The longer you live in two systems, the greater your chances of failing."

Break down barriers

If you do all of the hard work up front, you'll more than likely enjoy a successful project. But maybe you didn't man-

age a few of the steps quite right and you're facing a stalled project. "Don't give up," said Ordway. "There's still hope."

Even for an implementation gone sour, some processes probably worked well. Recognize what new solutions you tried and build on what has been working well, said Ordway. These are four strategies for reviving a failed or stalled implementation:

1. Assess the project. As part of assessing a stalled implementation, review what worked well and what didn't. Prior to starting the project, check to see whether your organization followed its road map. If not, you've immediately identified the steps you should add to your project when you revive it.
2. Celebrate the benefits. Even in a failed implementation, at least one new process or idea will work well. Take the time to evaluate any good that has come from the project and think about why that particular aspect worked. Then see whether you can apply the same implementation strategy to other areas of the project. Celebrating your success will also help boost morale.
3. Break down barriers. It's a bad idea to start up again with a huge new project, said Ordway. Instead, devise a small, focused plan that allows you to make progress and see the results of your success. At this stage, evaluate your top business needs. For example, draft a 30-, 60-, and 90-day plan. This refers to breaking down your project into mini-projects to complete in 30, 60, or 90 days. "These time frames are short enough that your team can remain focused and achieve a goal—whatever the goal of your mini-project is," said Ordway. "Especially with reviving a stalled project, you want to be able to see some positive results quickly. So, creating 30-, 60-, and 90-day plans will help with that."
4. Go for a quick win. Quick wins are similar to the 30, 60, and 90 day plan. Focus on determining what you can accomplish in a very short period of time to benefit your organization. If your project is stalled, there is probably a fair amount of frustration within the facility, so figure out what you can do quickly to show success. This quick win will help foster a more positive attitude about trying again. ■



Healthcare system trains 11,000 in 18 months

Learning and communication are the core of facilitywide implementation

Editor's note: This article is the second in a two-part series.

Evanston (IL) Northwestern Healthcare (ENH) is an integrated, academic healthcare system comprised of three hospitals, 851 beds, and 65 group practices. When ENH decided in 2001 to go electronic, training was a major part of the initiative—and it involved nearly 11,000 staff members. Luckily, ENH had Chief Learning Officer Jane Dowd to lead the effort.

"I was invited to a meeting to hear about a new 'tool' that ENH purchased," says Dowd, who has 20 years of training experience and a master's degree in education. "I didn't know until then that [the administration] was looking at me to lead the education portion."

The tool, of course, was an EHR. Dowd admits feeling a giant pit in her stomach when she first heard the news. "I had never done anything of this magnitude before," she says. "I only knew how to use Microsoft." Not to mention, she got the news a mere 12 months before the EHR was to go live. But once it sank in, Dowd and her team were determined to get the job done.

By the time ENH went live with its EHR, it had fully implemented its software education and communications initiative, which included the following:

- ▶ Eight training subjects
- ▶ 55 different courses
- ▶ 12,382 training encounters

The training initiative was a huge success. Now, with the staff up to speed on using the EHR, entire categories of medication errors, such as those due to illegible handwriting, have disappeared.

Reported medication errors have dropped. In another quality measure, the EHR reduced the time that it takes to deliver the first antibiotic to a patient.

ENH is also saving \$12 million per year with more effective and accurate registration and billing, says Dowd.

Don't underestimate learning

Many facilities don't realize that learning is one of the most expensive pieces of the entire implementation, says Dowd. You have to factor in supplies, hardware, and staff members' time away from their work. "In some cases, learning is more expensive than the software itself."

Practices and hospitals spend so much time evaluating vendors and choosing the perfect software that they sometimes

neglect the "what happens next?" part, which is crucial, says Dowd.

Your organization may never ask you to head up a training program as large as ENH's. However, regardless of how many people you need to train, a good program design will get you the results you want.

"Many facilities don't realize that learning is one of the most expensive pieces of the entire implementation."

—Jane Dowd

Start at the beginning

When you start any project, don't dive right in without making a solid plan. First, ask questions:

- ▶ What is the scope of the required training (e.g., content, level of complexity)?
- ▶ Who is the audience (e.g., past experience, job needs, biases, computer skills, learning preferences)?
- ▶ How many employees need to be instructed?
- ▶ What resources are available to me (e.g., trainers, facilities, computers, online resources, manuals, quick reference guides)?

Gather this information from managers, administrators, and other stakeholders whose staff and departments will directly feel the change the EHR brings—for example, IT, nursing, billing, and operations.

Set up meetings with your resident experts to discuss

what they know. Also talk to people one-on-one, observe staff members, and take a second look at job descriptions.

Once you've gathered your information, write down your learning objectives and how you will measure them, says Dowd. These objectives will serve as the road map for your training.

Then, think about the best way to teach employees. Adults prefer "just-in-time" learning, says Dowd. "They're practical—they want to know how information will help them in their day-to-day duties." Adults want to know what's in it for them. Think about how you operate in your job. You want need-to-know information in an easy-to-read format. "Quick reference guides and visually appealing, easy-to-read self-study resources are some of our most popular learning tools," she says.

In her own project, Dowd and her team knew quick reference guides would not be enough for the overwhelming scope of the EHR system. She also couldn't use online learning because the software was still rapidly changing. So she decided on instructor-led courses, supplemented by other tools such as newsletters, a CD-ROM, e-learning modules, and individual coaching.

Build the program

The next step is producing the curriculum you're going to teach and the course materials you're going to use—the quick reference guides, online courses, classroom-style courses, training manuals, overheads, etc.

ENH had to teach 7,500 employees and 1,600 physicians. It also had to accommodate more than 400 rotating house staff members and hundreds of types of users. To meet these needs, the hospital developed 55 classes from scratch. The training department partnered with almost 60 staffers, including nurses and billing professionals, to help design and teach the courses.

Before staff members began developing and teaching courses, ENH required them to complete an intensive six-to eight-week course on the system and pass exams proving their expertise.

They also had to successfully complete a "train-the-trainer" course to understand how adults learn and hone

their training delivery skills. In all, ENH ran training 15 hours a day, seven days a week, for six months, training nearly 11,000 people.

Because developing a complete training course can be so overwhelming, you can try using standardized document templates. This way, all materials will be consistent, and you can have multiple staff members develop materials that can fit together to form the complete education package. Content writers can then focus on the actual material, not the design.

Dowd says that your materials need visual appeal. "People generally felt too busy to read [instructional materials] and can easily get lost. They make split-second decisions as to whether to give something their attention, based upon the visual quality of a document. This can make or break your learning investment," she says.

Next, you'll need to select your trainers. A bad instructor can negate your well-thought-out materials and planning.

"Not everyone is meant to be a classroom trainer," says Dowd. Find trainers who come across as confident, credible, and professional. "Our trainers practice their introductions over and over," she says.

Mandate training

You can have the best materials and the best instructors, but those two factors won't train staff members unless you make training mandatory.

To emphasize training's importance, ENH required employees to take an average of 16 hours of training. The physician professional staff had to take 16–24 hours of training, even for affiliated physicians, says Dowd.

All users then had to pass a proficiency test, administered a few weeks after training. If they didn't score at least 85%, they wouldn't receive a password, and thus, couldn't use the system. Because system use was mandatory, no password meant they couldn't do their jobs at ENH.

This approach showed that ENH meant business when it came to the EHR—and that it would continue to maintain its high standards. Dowd credits this success to strong leadership support. ■

OIG audits

< continued from p. 5

concerns that you overlook the technical weaknesses in your environment. Look at the entire picture—from Web applications to operating systems to unstructured files scattered about the network.

4. Take action based on the vulnerabilities you uncover in your risk analysis; prioritize your weaknesses and focus on the most pressing matters.

“You can’t tackle everything at once,” Beaver says. “Where are you bleeding? Work on fixing what’s urgent and what’s important to help stop the bleeding and gain control of your environment.” Keep track of where you’re storing electronic PHI—both within the internal electronic environment and externally through remote devices and storage media. You’ll be surprised at where ePHI can end up, Beaver says. It’s in database query log files, temporary files, and word processing documents that users have copied to their local systems and left there.

Consider possible OIG approaches


In addition to the security rule, Parmigiani thinks the OIG might base its audits on the National Institute of Standards and Technology’s (NIST) SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. The guide is intended for government agencies and contains

more detailed information than the security rule, including a series of security-related activities to undertake and audit questions to ask. (You can access the NIST guidance at <http://src.nist.gov/publications/nistpubs/>.) Parmigiani says the following are areas on which the OIG might focus:

- ▶ Access controls (What is your setup? Do you have role-based access controls?)
- ▶ Contingency plans (Do you have one?)
- ▶ Audit and change controls (How do you manage these areas?)
- ▶ Experience in responding to past security incidents (What documentation do you have? How did you respond or mitigate?)
- ▶ Overall security program administration (Who is your information security officer? What are your policies and procedures? Is there separation of duties?)

“It’s a series of commonsense questions,” Parmigiani says. “You’d think that most hospitals by now could answer them accurately. But because HIPAA privacy and security haven’t been emphasized from an enforcement perspective, many providers have back-burnered compliance.”

Expect the OIG to give you the chance to agree or disagree with its findings, Parmigiani says. “Then, eventually, because the enforcement arm is CMS, the information will go to CMS.” ■

| EHRB Subscriber Services Coupon | | | | |
|---|-------------------|---|----------|-------|
| <input type="checkbox"/> Start my subscription to EHRB immediately. | | | | |
| Options: | No. of issues | Cost | Shipping | Total |
| <input type="checkbox"/> Print & Electronic | 12 issues of each | \$279 (ERBPE) | \$24.00 | |
| <input type="checkbox"/> Electronic | 12 issues | \$279 (ERBE) | N/A | |
| 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, CT, FL, GA, IL, IN, KY, MA, MD, MI, MN, NC, NJ, NY, OH, OK, PA, RI, SC, TN, TX, VA, VT, WA, WI. State that taxes products only: AZ. Please include \$27.00 for shipping to AK, HI, or PR. | | |
| Mail to: HCP Pro, P.O. Box 1168, Marblehead, MA 01945 Tel: 800/650-6787 Fax: 800/639-8511 E-mail: customerservice@hcpro.com Web: www.hcmarketplace.com | | | | |

| | | |
|---|---------------|-----------|
| 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 | | |
| Signature _____ | | |
| (Required for authorization) | | |
| Card # _____ | Expires _____ | |
| (Your credit card bill will reflect a charge to HCP Pro, the publisher of EHRB.) | | |



Delaware makes history with first RHIO go live

The Delaware Health Information Network (DHIN) went live in March with lab, radiology, and admission-discharge-transfer reports for three hospital systems, five practices, and the Laboratory Corporation of America. Considering that the DHIN just announced the RHIO in mid-November, implementation is moving along quickly.

The DHIN is running on a \$4.7 million grant from the Agency for Healthcare Research and Quality, \$2 million from the state government, and \$2 million from the three hospital systems, LabCorp, and Blue Cross Blue Shield of Delaware. The commission chose Medicity of Salt Lake City, partnered with Perot Systems, as the technology suppliers for the DHIN.

The Medicity/Perot team also recently won a contract to build an RHIO in California.

During the next phase, DHIN will develop its record-locator system.

Santa Barbara pulls the plug

Santa Barbara, CA-based County Care Data Exchange has ceased operations. Albert Kwyi, CIO at Cottage Health System in Santa Barbara talked about the data exchange's demise during a session at the February Healthcare Information and Management Systems Society conference in New Orleans. This announcement was news to many attendees.

The data exchange's governing body folded on December 31, 2006. Political—not technical—challenges were behind the downfall, Kwyi said.

This project had gained notoriety because of its early association with David Brailer, MD, PhD, the former national coordinator for health IT. Unresolved problems around data ownership and privacy weighed down the effort, said Kwyi.

Kentucky hospital quality data now available

The state of Kentucky launched a Web site where consumers can find data about the quality of care at Kentucky hospitals, reports *The Louisville Courier Journal*.

The online Health Care Information Center houses information such as how often patients die in a particular hospital while being treated for heart attacks, strokes, and other conditions.

The site also provides links to other hospital-comparison sites, including the Kentucky Hospital Association's listing of median prices at hospitals for various procedures.

Canada boosts health IT budget by \$400M

The Canadian federal government last week announced an additional \$400 million in funding for the Canadian health information network, *The Vancouver Sun* reports.

Canada Health Infoway is working to improve the storing and sharing of EHRs among clinics, hospitals, pharmacies, and other health facilities.

Canada Health Infoway already receives \$1.2 billion annually.

The largest portion of the additional government funding is for a three-year, \$612 million program for provincial and territorial governments to adopt guaranteed patient wait times, which means facilities will care for patients with critical health needs in a specific amount of time.

The budget supplement also includes an additional \$22 million for the Canadian Institute for Health Information to improve and expand wait-time data.

With the additional funding, the institute will now receive \$57 million annually. ■

Questions? Comments? Ideas?

Contact Managing Editor
Andrea Dickey, CPC-A

Telephone **781/639-1872, Ext. 3856**

E-mail adickey@hcpro.com



Physicians are blogging for better healthcare

Healthcare professionals are busier than ever with more patients and more computer skills to learn. But they're up for the challenge.

In fact, a growing number of medical professionals are seeking a creative outlet as amateur writers. And they're writing about their experiences with EHRs.

How? They blog. Also known as Weblogs, blogs are online publications that allow anyone with Internet access to become an instant publisher.

Content can range from personal thoughts—similar to a diary—to news, analysis, and political rants.

Blogging's popularity has grown exponentially since the first blogs launched roughly a decade ago.

Popular blog search engine Technorati tracks more than 40 million blogs and estimates that someone creates a new one every second. In fact, you might be surprised at how large and vocal the blogging community is.

Kevin Pho, MD, an internal medicine physician at Nashua (NH) Medical Group and author of the popular medical blog *Kevin, M.D.*, estimates that there are currently 500–1,000 blogs by physicians and other healthcare workers. Physician bloggers typically write about medical studies or hot topics in healthcare (e.g., technology, Medicare reimbursement, etc.), and their writing styles range from lengthy rants to short headlines with links to interesting news items.

A family physician who writes under the pseudonym **Sydney Smith** launched one of the pioneering physician blogs, *Medpundit*, in 2002.

Smith says she began blogging to express her opinions about healthcare topics in the news and to release frustrations over misinterpretations of medical studies.

Because it is relatively easy to set up a blog—by using free blogging software from Web sites such as *www.Blogger.com*, you can set up a blog in a few minutes for free—blogging has broken down barriers that previously prevented physicians from communicating with the public.

Now physicians can easily publish their writing for the entire world to see.

And because most blogging software allows readers to comment about what the authors write, they can also discuss their favorite topics with readers from around the world.

Medical blog readers often include other physicians, lawyers, and anyone else interested in healthcare.

"[There are] a lot of discussions between the physicians, so there's some pretty good debate that goes on," says Pho. ■

Blog it up: Get involved online and get answers

Here is a list of popular, helpful IT blogs. For more blogs, check out *www.hitsphere.com*. It lists more than 40 HIT-related blogs.

HIStalk—<http://histalk.blog-city.com>

This blog, launched in 2003, covers HIT news and opinion. You can also find interviews with healthcare whistleblowers, such as Justin Deal from Kaiser Permanente. (Deal sent out a mass e-mail about an EMR crisis at Kaiser after the board ignored it. Kaiser CIO Cliff Dodd left right after Deal's e-mail went public.)

The Healthcare IT Guy—www.healthcareguy.com

Shahid N. Shah, the author of this blog, touts himself as an HIT evangelist. He's been a CEO, a chief architect, and a software engineer. He now reviews new products and discusses EHR functionality (e.g., search capability) and gives advice (e.g., how to develop your own MPI using open-source software).

EMR Update—www.emrupdate.com

EMR Update is an online community with blog links, forums, articles, chat groups, and resources. This site also lists EMR price comparisons. Registration, which is free, may be required to access portions of the site.