

Health Information

Compliance Alert

TIMELY NEWS & ANALYSIS ON HIPAA, E-HEALTH, PRIVACY, SECURITY & TECHNOLOGY

INSIDE THIS ISSUE

Patient Privacy
Outsourcing Security on Patient Privacy Can Be Helpful — If You Know These 5 Essential Truths . . . 26

Therapy
Occupational Therapists Get Their Own Piece of the EHR Pie 27

Privacy
Keep Your Remote Workers' Information Private With This Sample Document 28

Privacy
Sending PHI Via Email? Find out How to Make Sure It Stays Safe . . 29

Security Strategies
HIPAA Compliant Banks Can Save You Money 30

Compliance Tactics
Nip Security Problems In The Bud With Walkthrough Inspections. . . 30

Industry News
Will The Feds Use EHR Taxes To Raise \$20 Billion Healthcare IT Fund? 31

What Exactly Is A Medical Device? 32

We welcome your comments & suggestions!

Mail **Mary Compton**, Editorial Director, at: maryc@inhealthcare.com.

To subscribe or request help with your current subscription, call: 1-800-874-9180 or e-mail: subscribe@eliresearch.com.

CMS Forms

Start Preparing Your Software Systems to Get Ready for the HIPAA 5010 Form

► *Heed this advice from CMS reps on the new “universal claim format,” which takes effect in 2012.*

You’ve got over a year to prepare for using the new HIPAA 5010 form, but CMS wants you to get ready sooner rather than later.

On March 23, CMS reps confirmed what many practices had wondered — the HIPAA 5010 form will become Medicare’s new universal claim format starting next year, noted **Pat Brooks**, RHIA, senior technical advisor with CMS, during a March 23 Open Door Forum.

To get acquainted with the 5010 form and its nuances, CMS offered the following advice during a March 24 conference call. Read on for more on how to prepare for 5010.

1. The 5010 form is ICD-10 ready. The new form offers “infrastructure” preparation for ICD-10, whereas the current 4010A1 does not, said **Christine Stahlecker**, director of the division of Medicare Billing Procedures in CMS’s **Office of Information Services**.

Other enhancements that you’ll find on the new form include improved claims receipt, claims editing, and error handling by the MACs, Stahlecker noted.

The improvements will allow MACs to return claims that require correction earlier in the process, and will assign claim numbers closer to the time that the MAC receives the claim.

2. Mandatory compliance begins on Jan. 1, 2012. Internal testing by CMS will take place this year, and external testing will begin starting in January, Stahlecker said.

Providers will have all of 2011 to complete their transition to the new form, but “Medicare fee-for-service will be productionally ready on Jan. 1, 2011,” she noted.

3. Analyze your system software within the next year. Not only will the MACs have to adjust their systems to prepare for the 5010 form, but you’ll have to prepare as well.

CMS Forms cont. on p. 29

Patient Privacy

Outsourcing Security on Patient Privacy Can Be Helpful — If You Know These 5 Essential Truths

► **Learn these facts before you nail down your HIPAA plan with a consultant.**

You may be relieved to find a consultant who is willing to take over the overwhelming task of helping you protect the privacy in your medical records — but keep in mind that not all outsourced privacy protection companies are the same.

Case in point: The Federal Trade Commission (FTC) recently settled a lawsuit with LifeLock, Inc., a company that offered identity protection services. “According to the lawsuit, LifeLock claimed its service would protect consumers against all forms of identity theft, when, in fact, LifeLock offered only limited protection against only some forms of ID theft,” the FTC’s statement noted regarding its \$11 million settlement with LifeLock.

If you’d like help staying current with HIPAA privacy regulations, consider these tips before you outsource any of your privacy needs.

1. The government does allow HIPAA consultants. Practices that are gun-shy about asking for HIPAA help should know that there are no laws against hiring a consultant to protect your patients’ privacy.

“The HIPAA law does permit covered entities to use a consultant for hire as their privacy officer, or to generally advise them on HIPAA-related matters,” says

Abner E. Weintraub, who helped produce the original HIPAA Compliance Extension Plan for HHS and is now the president of **HIPAA Group, Inc.**, in Orlando, Fla.

2. HIPAA requires ongoing upkeep. Some HIPAA consultants may come to your practice, evaluate your needs, and get you HIPAA-compliant, but your work isn’t done at that point.

“Because the entire purpose of HIPAA is to protect patient information, it’s impossible to be a one-stop, one-time visit or relationship,” Weintraub says. “It’s the frontline employees who deal with patient information day in and day out, so even if a consultant comes in, wraps up a nice bundle of policies and procedures, and does everything HIPAA requires, all that is a snapshot in time and as soon as the consultant leaves, it’s up to the employees to protect the patient information from hackers, accidental disclosures, etc.”

3. Be wary of cookie-cutter contracts. If your practice employs 400, but the HIPAA consultant’s contract offers standard training for 10, consider a different company.

Consultants should look at your practice’s overall needs depending on your size, specialty, processes, and setup, and tailor your privacy plan to your needs.

Patient Privacy cont. on p. 27

Don't Miss A Single Issue — Subscribe Today!

- Yes! Enter my one-year subscription to **Health Information Compliance Alert** for just \$297.
 Extend! I already subscribe. Extend my subscription one year at only \$297.

Payment Information: Check Enclosed: \$ _____ (payable to Eli Healthcare)
 Bill my credit card MC VISA AMEX DISC Exp. Date _____
 Acct. # _____ Signature _____
 Bill me (please add a \$15 processing fee for all billed orders) P.O. _____

Name _____

Title _____

Organization _____

Address _____

City _____ State _____ ZIP _____

Phone _____ Fax _____ E-mail _____

To help us serve you better, please provide all requested information.

Mail, call or fax your order to:

Health Information Compliance Alert

Eli Healthcare
 PO Box 933729
 Atlanta GA 31193-3229
 Call: 1-800-874-9180
 Fax: 1-800-508-2592

Therapy

Occupational Therapists Get Their Own Piece of the EHR Pie

► *Look for electronic health records tailored toward OTs, thanks to a new licensing agreement.*

Occupational therapists are finally getting some special electronic health record (EHR) attention, thanks to a new partnership. For a while now, speech pathologists and physical therapists have had the option to use tailored electronic medical record and documentation programs from their national associations — and now it's occupational therapy's turn.

The American Occupational Therapy Association (AOTA) announced in early November a licensing agreement with **Cedaron Medical Inc.** to develop an electronic patient record and documentation system for the occupational therapy profession.

"AOTA will work with Cedaron to develop documentation templates for evaluations, assessments, interventions, and outcomes specific to occupational therapy practice," said AOTA President **Penelope Moyers Cleveland, EdD, OTR/L, BCMH, FAOTA.**

OTs will be able to customize the software, document all components of patient care, and track outcomes,

the release said. In addition, the system has tools for scheduling patients and communicating directly with billing systems.

Perk: Users participating in AOTA's National Outcomes Database for Occupational Therapy will be able to access national and facility-based outcomes measures for benchmarking.

The system will capture outcomes data using the **Boston University Activity Measure for Post Acute Care (AM-PAC™)** and other measures. The AM-PAC, an outcome instrument provided by CREcare, LLC, assesses a client's functional status across three domains: basic mobility, daily activities, and applied cognitive.

The AOTA documentation system will be compatible with ASHT Connect (specifically for hand therapists), SLP Connect by ASHA and APTA Connect, allowing for a common electronic platform across the occupational therapy, physical therapy, and speech language pathology professions, AOTA clarified. □

Patient Privacy cont. from p. 26

4. Don't forget the scope of identity theft. Your patients' personal health information (PHI) includes clinical records — as well as billing records, Social Security numbers, drivers' license copies, etc. — leaving patients open to a risk of identity theft. "Medical records have cash value to criminals, and there are underground marketplaces where PHI is bought and sold 24/7," Weintraub says. "Even L.A.'s notorious gangs have moved into the identity theft marketplace because it's slow to track and investigate."

5. Consider tracking and monitoring services. Once your HIPAA plan is in place, you might want to consider adding another layer of protection to ensure that you are covered if a breach ever occurs.

Even if you think a security breach could never happen at your practice, keep in mind that not all breaches

are deliberate. "I had a client who sent a fax that included PHI, and the fax went in error to the wrong place," says **Barbara J. Cobuzzi, MBA, CPC, CPC-H, CPC-P, CENTC, CHCC,** president of **CRN Healthcare Solutions.**

The practice contracted with a service that performs not only identity theft monitoring, but also takes the legal and investigative steps required to restore credit if it's been stolen. The practice offered the service to the patient whose privacy had been breached. "Certain companies, such as **Identity Theft Shield,** will give you the legal defense necessary to restore credit in these situations," Cobuzzi says. "I'd recommend a practice providing that type of coverage for all of its employees, and then if there's a breach, to provide it for the patients(s) whose security was breached." □

Comments? Questions? Concerns?

Mail to: **Sudeep Guha, Editor,** at: sudeepg@eliresearch.com

Privacy

Keep Your Remote Workers' Information Private With This Sample Document

► ***Make sure your offsite workers are aware of security and privacy concerns.***

Your practice has tough decisions to make when allowing employees to handle patients' private health information (PHI) while working from offsite locations. You may require encryption, you may prohibit them from working on their personal laptops when dealing with PHI, or you may even only allow remote work when it's done for emergency reasons. But no matter what, you need to communicate your privacy expectations to your employees.

Consider this sample document as a guide, contributed by **Glenn Allen**, information security director with **Fairview Health Services** in Minneapolis, Minn.:

Security Considerations/Guidelines for the Remote Worker: When working remotely, we expose [organization name] to increased risk of privacy and security incidents and breaches. [Organization name] takes great care in protecting the privacy and security of its paper and electronic systems in order to safeguard its patient (and other confidential) data. Remote workers need to take the same care.

- Only use a currently supported operating system (e.g., XP or Vista) with all available security patches.
- Use auto-updating antivirus software. Antivirus with outdated virus definitions has reduced effectiveness.
- Use a properly configured firewall. Also strongly consider having a properly configured router between your equipment and internet connection (which can greatly increase your protection as well).
- Be careful when using shared (family) computer equipment to access [organization name] resources. The computer you share can inadvertently be compromised by others. It may make sense to limit access to equipment used to connect to [organization name] unless you understand what others are using the computer for.
- Do not use any form of file sharing programs on equipment used to connect to [organization name] resources. Many file sharing programs can be used to open or share folders and files on your own computer

(sometimes without the user meaning to).

- Get guidance from your operating system vendor on safe computing. Many OS vendors (like Microsoft) have great resources for both end-user and IT professionals.
- Never reply to, open links in or attempt to unsubscribe to unsolicited emails. Just following a link in an email to a hostile site can compromise your computer.
- Immediately report any security concerns to your manager or the IT department.
- It is required that comprehensive steps be taken to make sure that only programs directly related to the employee's business purpose are run while being connected to [organization name]'s network.
- Position your monitor so that unauthorized person/s cannot view the screen.
- User ID and/or passwords may not be shared or written, taped or stored on the computer/laptop, in the computer bag or in any location relative to the computer.
- Be careful when printing confidential documents. Be sure you are printing to the correct printer and that you are able to retrieve any confidential documents quickly.
- Be aware when using wireless hotspots. Some wireless hotspots may be run by unscrupulous individuals who are looking to steal/misuse data and equipment connected to the hotspot.
- [Organization name] may inspect and monitor data and communications at any time. This includes monitoring network usage (including contents), and examining files on any system that has been connected to the network.
- Be mindful when selling or getting rid of computer equipment. Remember to scrub or properly dispose of drives (including flash/thumb) so others cannot access confidential data. □

Privacy

Sending PHI Via Email? Find out How to Make Sure It Stays Safe

► ***Look at alternatives to encryption when you deem them necessary.***

An email that contains a patient's protected health information (PHI) can be completely harmless — unless it falls into the wrong hands.

But fortunately, there are a few ways that you can head off potential email security breaches.

Although many practices have started encrypting their emails, you aren't specifically required to do so yet. The Aug. 24 *Federal Register* indicates that "a covered entity may be in compliance with the [HIPAA] Security Rule even if it reasonably decides not to encrypt electronic PHI and instead uses a comparable method to safeguard the information."

You may be wondering what might constitute a "comparable method," and why this is required in the first place.

The background: Any time you're sending a patient's PHI, whether it's via the internet or the mail, you have to ensure that it won't fall into the wrong hands. One way of protecting electronic communications is to install encryption software.

"Covered entities, such as physician practices, must undertake an assessment of their environment to determine whether encryption of electronic protected health information is reasonable and appropriate," says **Mark C. Rogers, Esq.**, with **The Rogers Law Firm** in Braintree, Mass. "If, after undertaking such an assessment, encryp-

tion is not reasonable and appropriate under the circumstances, a covered entity needs to document that determination and, if appropriate, implement an equivalent alternative."

In 2006, CMS issued guidance in which it recommended that all portable or remote devices that store electronic protected health information should employ encryption technologies of the appropriate strength, Rogers says.

Other alternatives: "You can password-protect your email, which is the simplest way to protect it," suggests **Barbara J. Cobuzzi, MBA, CPC, CENTC, CPC-H, CPC-P, CPC-I, CHCC**, president of **CRN Healthcare Solutions**. "Printing a document which contains PHI to an Adobe PDF and then protecting it with a password before attaching it to an email will ensure that the PHI is not easily accessible to anyone other than the intended recipient."

If you need remote access to an EMR (which outside billing companies often do), you can use a virtual private network (VPN) or a Citrix connection. "Citrix works because it only passes one keystroke at a time over the web, so if anyone intercepts it, they are seeing just one keystroke at a time," Cobuzzi says.

Bottom line: Find a method that works well for your practice and keeps your patients' PHI safe. □

CMS Forms cont. from p. 25

"Your systems that you are using to actually create the Medicare billing or receive and process the remittances, posting them to your accounts receivable systems, they will all need to change," Stahlecker said. "Some of these new versions have new data element requirements, so you should be studying up on these changes and understanding which business processes you may need to modify," she indicated.

4. Contact your vendors. Ask your system vendors whether your current software license includes regulatory updates, Stahlecker advised. If not, the vendor may require you to pay additional funding before they perform such upgrades.

You should also inquire to determine when your vendor plans to upgrade your system, and ensure that your transition will take place long before the Jan. 1, 2012 cut-off date, Stahlecker advised.

5. Say goodbye to P.O. boxes. "Please note that post office boxes are no longer permitted in a billing provider address," Stahlecker said.

This new regulation will take effect as soon as you begin using the 5010 forms. "It's mandatory when you stop using the 4010 format," Stahlecker said during the call. □

Security Strategies

HIPAA Compliant Banks Can Save You Money

► **Banks performing more clearinghouse functions, say experts.**

Partnering with your bank to process your practice's claims and other financial transactions can boost your practice's bottom line.

Tip: Financial transactions outside the healthcare industry are usually conducted for mere pennies. Compare that with the exorbitant rates the healthcare industry deals with and you see the allure. "Why shouldn't it be that a healthcare transmission costs pennies on the dollar instead of \$15 to \$20 per claims transaction?" asks **Matthew Rosenblum**, COO of **CPI Directions Inc.** in New York.

This cost efficiency is a major factor. If banks comply with HIPAA's regulations, the healthcare industry can both please their patients and improve their bottom lines. However, the future of banks and clearinghouses remains to be seen.

Disadvantage: If banks are declared exempt from HIPAA's regulations, clearinghouses could warp into banks to avoid HIPAA's rules and regulations. "It's not a far-fetched notion that banks and clearinghouses will begin to

merge if it's advantageous," says **Anna Slomovic**, a senior fellow at the **Electronic Privacy Information Center (EPIC)** in Washington, DC.

"That would be a logical move for [clearinghouses] under those circumstances," asserts **Debbie Larios**, a partner in the Nashville, TN office of **Miller & Martin**. Though, with all the regulation already directed toward banks, "it's more likely that they would cry foul that the banks would get undue advantage," she predicts.

As the issue is hashed out among industry regulators, providers can take steps to protect their patients' privacy via the BAA.

Problem: Most agreements require that business associates facilitate similar contracts downstream, but those sections are very truncated, Larios explains.

Solution: Go into detail and expand the language in your BAA so that business associates can understand, appreciate and abide by HIPAA's rules, Larios suggests. □

Compliance Tactics

Nip Security Problems In The Bud With Walkthrough Inspections

► **Follow this advice to keep your compliance plan in shape.**

Your security compliance program could be long overdue for a checkup.

Now is the time to begin monitoring your staff so you can knock out compliance violations before they occur. Here's how to get started:

Recruit Anonymous Reviewers

The basics: Much like the safety audits your office already performs, a walkthrough can prevent violations before the Department of Health and Human Services gets involved. Whether inspections are announced or executed without your staff's knowledge, experts agree that they should be done at least annually for all departments and more often for high-risk areas.

"If you've found a problem area, then you want to do [walkthroughs] more often than [once a year] to get things really ironed out," suggests **Patricia Johnston**, a consultant for **Texas Health Resources** in Arlington, TX.

Though not mandated by the privacy rule, third party or anonymous reviewers are often an efficient,

if costly, method of examining your facility's HIPAA compliance program. "The big thing is making sure that nobody knows what's going to happen because you want to see what people are doing on a day-to-day basis, not what they're doing on their best behavior," posits **Robert Markette**, an attorney with Indianapolis' **Gilliland & Caudill**.

The types of violations often caught in walkthroughs range from simple mistakes — like leaving confidential faxes unattended or discussing PHI in public areas — to trickier situations that may have been overlooked. Many times the problem is not a procedural violation, but an issue that hasn't been thought through all the way, Markette says.

Focus On Your Frontlines

"Focus on [areas with] a significant amount of interaction with the public or ... patients," advises **Brian Gradle**,

Compliance Tactics cont. on p. 31

Industry News

Will The Feds Use EHR Taxes To Raise \$20 Billion Healthcare IT Fund?

► **Medical device tax could pose big costs for consumers.**

Now that the \$787 billion **American Recovery and Reinvestment Act of 2009** (ARRA) includes approximately \$20 billion for healthcare IT, the administration is getting ready to throw a lot of money around. Seems funny but not many have yet mulled where the \$20 billion will be coming from, the source of which could be a new tax on medical devices that hasn't come into the spotlight yet. In a blog-post on www.healthdatamanagement.com, editor-in-chief of the Web site **Greg Gillespie** talks about this new tax — a 2.3 percent excise tax on medical devices set to go into effect in 2013. Gillespie says this figure probably

didn't get much exposure in the media because it doesn't sound like much, unless you're in the medical devices market. But the tax could generate almost \$2 billion every year, says Gillespie.

Consumers to Bear the Cost Burden

Expert opinion, says Gillespie, is that medical device manufacturers will try to find ways to pass the costs on to the consumers, the middlemen, and device suppliers.

Industry News cont. on p. 32

Compliance Tactics cont. from p. 30

an attorney with the D.C. office of **Hogan & Hartson**. Waiting rooms, elevators and even fax machines are all areas where information can accidentally be heard or viewed by the public, Gradle offers.

Example: In a walkthrough, Markette noted that though the office had obviously positioned computer monitors so that they could not be seen from the waiting room, staff members hadn't considered the glass entryway to be an area of risk. "As you walked in, you could look right over the employee's shoulder," he observed.

"Any time a privacy official is walking through, they should have their eyes and ears open," claims Gradle. However, experts agree that while privacy officials should conduct informal walkthroughs frequently, there must be some method to document and track violations, and there must be follow-ups.

To solidify the process of monitoring HIPAA compliance, Johnston developed a walkthrough checklist. As a tangible record of violations, the checklist should be based on the privacy policies and procedures central to your organization. It can also include how many times the violation was observed. "It gives you something to start tracking to see if you see any improvement or not," Johnston explains.

The next step: Once you've performed the walkthrough and logged the violations, compliance officers and others can review the document to see what went wrong and where. "The two main areas we look for are our training and the clarity of our policies," Johnson points out. If a

violation is observed multiple times, you have to ascertain the causes behind it.

By pinning down answers to these questions, you can streamline your facility's procedures, and thereby avoid glaring HIPAA violations.

Get Tough And Enforce Sanctions

Tip: Remember to take HIPAA violations seriously, if and when they do occur. That means you'll have to outline and impose sanctions according to the gravity of the violation. Not only does failure to apply penalties jeopardize your compliance program — it's also against the law not to have a sanctions policy in place.

Following your sanctions policy will benefit you in the long run, Markette explains, as it proves to your employees the importance of maintaining privacy standards, while at the same time preventing them from using past inconsistencies to excuse or eliminate their responsibility to protect health information.

Word to the wise: To correct the problems encountered during the walkthrough, experts concur that it is best left to the discretion of the privacy officer to determine how and when a sanction will be imposed. Usually, that officer complies with the overall HR sanctions policy; however, as the issues move in the direction of malicious and willful breaches of privacy, higher levels of sanctions — including termination — must be applied. □

Industry News cont. from p. 31

Whichever way the cookie crumbles, it's the end consumer whose arm is going to get twisted. (For a reality check, visit: www.cleveland.com/medical/index.ssf/2010/04/health_care_fact_check_the_imp.html.)

Excise taxes like these, according to Gillespie, have almost always seen indiscriminate use of taxes, fees, unfunded mandates, etc., to shift money from here to there. And this time he says EHRs are being perceived as the backbone of a potential national health infrastructure that will use health information exchanges to plug everyone — patients, provider, insurers, government health agencies, etc. — into one mammoth-sized health entity that will definitely need sustainable revenue streams.

This could result in, the blog goes on to say, someone in the system deciding that because there's been an artificial expansion in the EHR market on account of the HITECH Act, and because the EHR market has some deep-pocketed players in it, the EHR market should pitch in its contribution in the form of a tax on their products.

But Are EHRs Medical Devices?

Gillespie says that taxing EHRs is something feds have been attempting for some years and now they finally have a foot in the door. The **Food and Drug Administration (FDA)** has been trying for quite some time to add EHR regulation to its host of responsibilities. If it succeeds this time, electronic records will fall into a new category that will make it easier to target.

Gillespie further says in the post that in February 2008 the FDA had made some noise by issuing a proposed rule for regulating medical device data systems (MDDS), defined as software that transfers, displays, reformats or stores data from a medical device without acting upon that device. The rule proposed to classify MDDS as a Class 1 medical device, the lowest risk category.

Industry players are trying to fight back, but the writing on the wall is quite clear. It is just a matter of time before an EHR tax rears its head — whether the entry will be through the front door, or it'll be stealthier in the form of a medical device tax remains to be seen, says Gillespie in his blog-post.

(**Editor's note:** Greg Gillespie's post on www.healthdatamanagement.com/blogs/blog_Gillespie_EHR_tax_FDA_healthcare_regulation_federal_reform-40110-1.html.) □

What Exactly Is A Medical Device?

Technically speaking, the FDA defines a medical device as: an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them. (The complete definition of Medical Devices can be read at: www.en.wikipedia.org/wiki/Medical_device#Definition_in_USA_by_the_Food_and_Drug_Administration.)

Customer Service:

(800) 874-9180

Mary Compton, Editorial Director

(919) 647-9569

Jeanne Caggiano Publisher

(919) 281-0474 ext. 316

Bulk Sales:

(888) 463-3608

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Health Information Compliance Alert™ (USPS 022-061) (ISSN 1548-985X) is published monthly by Eli Research, Inc. 2222 Sedwick Rd, Durham NC 27705 with editorial offices at PO Box 90324, Washington, DC 20090-0324. Periodicals Postage is paid at Durham, NC and additional entry offices. Annual subscription price is \$297.

Postmaster
send change of address to
Health Information Compliance Alert, PO Box 413006,
Naples FL 34101-3006.
© Eli Research.