



Health Information Compliance Insider®

A PLAIN-ENGLISH GUIDE TO HIPAA REGULATIONS

HIPAA in the headlines in 2009

Anticipate impact in 2010

The quality, efficiency, safety, and privacy of health-care in the United States were front-page news in 2009.

Specific developments weren't mere flashes in the pan; experts say the ripple effect will continue into 2010 with long-ranging effects for most.

HICI revisits the most significant events of 2009 and explores their potential effect in 2010.

HITECH Act

► **The development:** The Health Information Technology for Economic and Clinical Health (HITECH) Act, which was signed into law February 17, 2009, is one provision of the American Recovery and Reinvestment Act of 2009. The HITECH Act aims to promote use of federal stimulus money to advance the design, development, and implementation of a nationwide health information infrastructure that promotes the use and exchange of information via electronic health records (EHR).

IN THIS ISSUE

p. 4 Red Flags update
Yes, the FTC has delayed enforcement again—the fourth time it has done so.

p. 6 Identity theft prevention
The government will be coming at you from all angles to ensure compliance with patients' information. Are you ready? Here are some steps on how to prevent breaches and handle them should they occur.

p. 7 2009 index
See a list of articles that have appeared in **HICI** in 2009.

HICPro

Congress included stiffer penalties for noncompliance with HIPAA, greater breach notification requirements, and expanded enforcement to address growing privacy and security concerns. For example, business associates (BA) now must comply with the HIPAA security rule and HITECH's security provisions.

Rebecca Herold, president of Rebecca Herold & Associates, LLC, in Van Meter, IA, calls it one of the most significant developments.

"There are many times more business associates than there are covered entities," Herold says.

Covered entities now must notify HHS of any breaches no later than 60 days after

The CVS fines made clear that [the government] now operates under a sort of "zero tolerance" policy.

learning of them. They also must notify prominent media outlets in the state when a breach affects more than 500 individuals.

► **What to do about it now:** HHS will begin enforcing the amended breach notification provisions by around February 22. Covered entities must fine-tune their processes now.

"This means that all personnel, volunteers, and agents need to know what to do if they discover a data breach," says **Rebecca L. Williams, Esq., RN**, partner at Davis Wright Tremaine, LLP, in Seattle.

Covered entities must amend their BA contracts by February 18. Organizations should work with their legal department to revisit existing contracts and ensure that they have the proper template for new ones.

Incentives for meaningful use of EHRs will begin in 2011. Congress wants stakeholders to purchase and implement EHRs in 2010 to prepare for 2011. However, stakeholders may be slow to react because of up-front costs.

> *continued on p. 2*

Anticipate impact

< continued from p. 1

“The push for healthcare providers to go paperless has created more electronic health records and repositories than ever before,” says Herold.

Take time to determine the timetable and EHR option that are cost-effective for your organization.

Major pharmacy company fined for breaches

► **The development:** On February 18, 2009, HHS and the Federal Trade Commission (FTC) fined CVS Caremark Corp. \$2.25 million for inappropriate disposal of PHI. An investigation of CVS’ practices followed reports that the company discarded patient information in industrial trash containers outside some of its stores. CVS failed to secure the containers, making the PHI accessible to anyone, according to HHS.

The privacy rule requires health plans, healthcare clearinghouses, and most healthcare providers (covered entities), including most pharmacies, to safeguard the privacy of patient information, even during its disposal.

Specifically, HHS said CVS violated the privacy of millions of its customers when it:

- Failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process
- Failed to adequately train employees to discard such information properly

► **What to do now:** The CVS fines made it clear that HHS and FTC (and now OCR) now operate under a sort of “zero tolerance” policy. The fines also served as a warning that anyone violating the privacy rule is subject to substantial fines and embarrassment.

Pursuant to the HITECH Act, HHS issued guidance April 17, 2009, requiring providers to shred or destroy any paper, film, or other hard-copy media to ensure that no one can read or reconstruct the PHI.

Celebrity privacy cases publicized in California

► **The development:** The problem of curious hospital workers who snoop inappropriately in medical records has long existed. During the past few years, it has become news as well. Celebrities, angry because healthcare workers have sold their information to tabloids, have fought back in California’s newspapers and state legislature.

Notable cases involved the late Farrah Fawcett in 2007 and Britney Spears in 2008. These high-profile cases inspired a bill that Governor Arnold Schwarzenegger signed into law January 1, 2009. The new law permits the state to impose heavy financial penalties (as much as \$250,000) on healthcare providers who inappropriately peek in patients’ medical records.

It didn’t take long for the state to flex its newfound muscle. State regulators slapped the maximum penalty on Kaiser Permanente’s Bellflower (CA) Hospital in May 2009. Regulators found that Bellflower failed to

Editorial Advisory Board

Health Information Compliance Insider®

HCPPro

Group Publisher: **Lauren McLeod, CPC-A**

Executive Editor: **Ilene MacDonald, CPC**

Sr. Managing Editor: **Dom Nicastro, dnicastro@hcpro.com**,
781/639-1872, Ext. 3413

M. Peter Adler, Esq.

Foley & Lardner
Washington, DC

Chris Apgar, CISSP

Apgar & Associates, LLC
Portland, OR

Mary D. Brandt, MBA, RHIA, CHE, CHPS

Brandt & Associates, Inc.
Bellaire, TX

Todd C. Brower, Esq.

Wolf Block Brach Eichler
Roseland, NJ

Karen G. Grant

Partners HealthCare
Systems, Inc.
Chestnut Hill, MA

Tom Hanks

Health Care Strategy & Change
IBM Business Consulting Services
Chicago, IL

Gwen Hughes, RHIA, CHP

Care Communications
Chicago, IL

Kelly A. Moore

Cogent Healthcare, Inc.
Daytona Beach, FL

Leigh-Ann Patterson-Durant, Esq.

Nixon Peabody, LLP
Boston, MA

Michael C. Roach, JD

Meade & Roach, LLP
Meade Roach Consulting, LLP
Chicago, IL

Frank Ruelas, MBA

www.hipaabootcamp.com
Scottsdale, AZ

Edward Shay, Esq.

Post & Schell, PC
Philadelphia, PA

Jonathan Tomes, Esq.

Tomes & Dvorak
Overland Park, KS

Health Information Compliance Insider® (ISSN: 1531-6009 [print]; 1554-0448 [online]) is published monthly by HCPro, Inc., 200 Hoods Lane, Marblehead, MA 01945. Subscription rate: \$249/year; back issues are available at \$25 each. Copyright © 2010 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. Please notify us immediately if you have received an unauthorized copy. 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 **Health Information Compliance Insider**. 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. **Health Information Compliance Insider** is not affiliated in any way with The Joint Commission, which owns the JCAHO and Joint Commission trademarks.

prevent employees from snooping in the medical records of Nadya Suleman, who gave birth to octuplets in January 2009.

➤ **What to do now:** These high-profile cases cast a spotlight on inappropriate behavior in hospitals and pressure all providers to improve their processes. Conduct a risk assessment to determine whether your organization is vulnerable. Consider strategies such as monitoring system access logs or using “honeypots” to catch snooping staff members.

“It’s important for organizations to work harder to eliminate and detect snooping when workers look at the medical records of people they have no business looking at,” says **Michael C. Roach, Esq.**, of Meade & Roach, LLP, in Chicago.

But this is no easy task.

“It is probably technologically impossible to prevent all snooping,” says Roach—meaning the odds are stacked against you.

OCR became responsible for HIPAA security rule enforcement

➤ **The development:** HHS announced July 27, 2009, that it would transfer HIPAA security rule oversight from CMS to OCR. CMS had overseen the rule since it became effective in 2003.

➤ **What to do now:** Be prepared for greater enforcement of the HIPAA privacy and security rules; they both now fall under OCR’s umbrella. It is likely no coincidence that a plan for increased penalties for privacy and security violations is part of the HITECH Act that was enacted only four months earlier.

OCR now will evaluate whether HIPAA security standards preempt any state laws, impose financial penalties for violations, and issue subpoenas pertaining to security violations, according to HHS.

Meaningful use—evolving definition, application, and timetable

➤ **The development:** In mid-July 2009, the Health IT Policy Committee approved a work group’s

revised recommendations for defining the meaningful use of EHRs. This was the first step in a federal Medicare and Medicaid program that uses incentives to require physicians’ and hospitals’ financial commitment to EHRs.

HHS was expected to release a proposed rule in December.

The final definition of meaningful use could lead to:

- Easier exchange of patient information when necessary
- Greater availability of patient information
- Appropriate data and transmission security
- Better quality of care
- Greater efficiency

The work group also recommended that providers allow patients to access their personal health records by 2013. Its initial recommendations proposed patient access by 2015.

The new recommendations also require all providers to participate in a national health data exchange by 2015.

“The verdict is still out on how beneficial the final definition of meaningful use will be to healthcare,” says **Chris Apgar, CISSP**, president of Apgar & Associates in Portland, OR. “It can have great value, and it can also hamper [health information technology] adoption if it is too expensive, requires too much, and/or is not well thought out.”

➤ **What to do now:** Privacy and security officers must do more than conduct research and prepare to implement EHRs. They also should prepare to strengthen their policies because violations may directly affect EHR incentives and reimbursement. The work group recommended that CMS withhold incentive payments until a provider resolves any pending HIPAA violation charges.

Meanwhile, providers must demonstrate meaningful use by ensuring that their EHRs:

- Allow patients to access their own health records quickly

> *continued on p. 4*

Anticipate impact

< continued from p. 3

- Implement at least one clinical decision support rule for a specialty or clinical priority
- Provide patients electronic copies of discharge instructions and procedures
- Exchange health information where possible
- Submit insurance claims electronically
- Verify insurance eligibility electronically when possible ■

Red Flags rules

FTC enforcement date finally arrives ... at least for now

The Federal Trade Commission (FTC) now says it will enforce the Red Flags rule June 1, seven months after its previous deadline of November 1, 2009.

Nonetheless, providers subject to the rule's requirement to develop a program that mitigates the risk of identity theft within their organizations must establish their programs now. (See p. 6 to learn how to create an identity theft prevention program.)

"As with the [Health Information Technology for Economic and Clinical Health] Act's enhanced privacy and security requirements, some hospitals are completely on board, but others are lagging," says **Kate Borten, CISSP, CISM**, Marblehead (MA) and Associates. "I think the reasons are usually a combination of lack of resources, such as people and money, and lack of a high-level leader taking a strong stand."

Further, many hospitals don't see themselves as creditors and are slow to comply, says Borten. The FTC requires entities it defines as creditors to comply with the rule. Pursuant to the rule, organizations that allow patients to defer payments for services are creditors.

"There is still reluctance and opposition to its application to various industries and various size workforces and operations," says **John C. Parmigiani**, a HIPAA security and privacy consultant and president of John C. Parmigiani & Associates, LLC, in Ellicott City, MD. "Consequently, there will be foot-dragging on the enforcement front while the rule is still being debated."

Still, the FTC expects strict compliance, as evidenced by the extra time it is allowing. The original compliance

date was November 1, 2008. The FTC then delayed it until May 1, 2009, and yet again until August 1, 2009. The FTC may levy penalties as high as \$2,500 for each independent violation of the rule, says Parmigiani. The rule authorizes state attorneys general to recover \$1,000 for each violation and court fees.

Nuts and bolts

The FTC developed the Red Flags rule pursuant to the Fair and Accurate Credit Transactions Act of 2003. The rule requires financial institutions and creditors with covered accounts to establish identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

"I still believe the major determinant is whether the provider is a creditor, not its size or if it knows everybody that it deals with, which is the proposed basis for exemption," says Parmigiani. "But of greater concern is how it is protecting the digital information of the patient to whom it extends credit."

If you haven't already done so, meet with legal counsel to review patient records and billing policies and procedures to ensure compliance as soon as possible.

The rule identifies certain types of information necessary to verify identity, including identifiers such as the following:

- Name
- Social Security number
- Passport

- Tax identification number
- Biometric data such as fingerprint and voiceprint

Organizations not in compliance must quickly conduct an organizational audit to find potential problems, says Parmigiani. Allow sufficient time to conduct a thorough investigation, he says.

Next, develop a theft prevention program, which is an FTC requirement. This is necessary to track every account.

The written program must satisfy all of the following criteria:

- Identify potential red flags within an organization
- Help detect red flags when they occur in real time
- Detail how an organization will respond to attempted identity theft (i.e., how to prevent it from occurring or how to mitigate the damage if it does occur)

These steps are necessary for compliance with the rule, but they're also important for maintaining good business standards, says Parmigiani.

"It is essential to moving ahead and to [becoming] fully operational in an e-health environment," Parmigiani says. "Protecting against identity theft and medical identity theft and ensuring data confidentiality, integrity, and availability are critical success factors in the trust equation [with your patients]."

Before a program goes live, the FTC also requires that organizations first obtain approval from their board of directors.

Let the HIPAA playbook be your guide

HIPAA requires covered entities to protect the integrity of their patients' information. The FTC requires creditors to have a program to help them do so with respect to specific information. Organizations certainly can parlay some of the work they've done with respect to HIPAA to develop training strategies for dealing with identity theft.

As with HIPAA, organizations must train staff members how to identify red flags and how to respond to them. The Red Flags rule requires them to do so, says Borten. "It's not trivial, but it's also not rocket science," she says. "You should just be building on your HIPAA privacy and security requirements. If you're a HIPAA-covered entity, there is certainly overlap."

Organizations need more than checklists, however. As with HIPAA, policy and procedure training and refreshers are necessary, says Parmigiani. Specifics are left to the organizations' discretion.

Don't focus solely on staff members. Organizations must consider vendors working on their behalf. "Bring them into the mix," says Parmigiani. "They are contractually bound to you and need to be on the same page as you." ■

HICI Subscriber Services Coupon				
<input type="checkbox"/> Start my subscription to HICI immediately.				
Options	No. of issues	Cost	Shipping	Total
<input type="checkbox"/> Print & Electronic 1 yr	12 issues of each	\$249 (HICIPE)	\$24.00	
<input type="checkbox"/> Print & Electronic 2 yr	24 issues of each	\$448 (HICIPE)	\$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 HICI.)				
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				

Responding to identity theft a three-step process

Privacy and security officers have more rules than ever before with which they must comply. The Federal Trade Commission's Red Flags rule, existing HIPAA laws, and the new Health Information Technology for Economic and Clinical Health (HITECH) Act require that covered entities:

- Protect patient information with technical, administrative, and physical safeguards (HIPAA)
- Lessen the negative effect of unauthorized disclosure (HIPAA)
- Notify patients within 60 days of breaches that involve unsecure PHI and pose a significant risk of financial, reputational, or other harm (HITECH)
- Inform HHS of breaches (HITECH)
- Establish an identity theft prevention program with policies and procedures to detect, prevent, and mitigate identity theft (Red Flags rule)

Implement a three-step process to protect all patient information that includes plans for what to do before, during, and after a security incident, says **Andrew E. Blustein, Esq.**, partner and cochair of Garfunkel Wild & Travis, PC's Health Information and Technology Group in Great Neck, NY, Hackensack, NJ, and Stamford, CT.

"A medical record is chock-full of information that an identity thief can use to its advantage," says Blustein. "It's basically a treasure chest of credit card numbers, Social Security card numbers, and everything else someone needs to steal an identity."

Before the breach

Mitigate harm resulting from identity theft by preventing breaches from occurring, says **David A. Mebane, Esq.**, senior vice president for legal affairs at Saint Barnabas Health Care System in West Orange, NJ.

"You want to create the right amount of technical safeguards so your patients are protected," says Mebane.

Safeguards include:

- Encrypting laptop computers and other portable devices

- Prohibiting the installation of unsecured software
- Creating system firewalls
- Establishing remote access roles specific to applications and business requirements
- Destroying unnecessary patient information
- Using and updating antivirus software

HHS also provides specific guidance for securing portable devices at www.cms.hhs.gov/securitystandard/downloads/securityguidanceforremoteusefinal.pdf.

Establish policies and educate employees and vendors about their responsibility to protect information and report incidents, says Mebane.

"You'll also want to perform regular audits so you have a way of detecting breaches," says Mebane. "Once the information has been stolen and is in the wrong hands, a lot of the damage will already have been done."

Create an incident response program, advises Blustein. Form teams and designate leaders responsible for responding to and investigating any breaches. Ensure that your policies specify:

- The type of information that must be reported
- The entities to whom information must be reported
- The deadline for reporting information
- Penalties for individuals responsible for the breach

Responding to the breach

"Installing a program to prevent loss of PHI is like putting an alarm on your house," says Blustein. "It's a good start and it will prevent some thieves, but it doesn't mean you'll never have a problem."

If you discover a breach, alert your attorneys and consider retaining outside counsel. This serves two purposes. It provides an unbiased look at the event and helps protect your organization.

Activate the response teams you previously established, says Blustein. They should be prepared to investigate all aspects of the breach, including:

- How the theft occurred
- Who took the information
- Whether employees were at fault
- The amount of information taken
- The number and identity of affected patients
- The type of information stolen

Soon after making these determinations, decide whom you must notify and how you must do this. You'll need to consider state law, HIPAA, and the HITECH Act, says Blustein. You also must ask yourself what the right thing to do is, he says.

"You need someone in your organization who can make these decisions quickly to avoid the bottleneck problem," says Blustein. "The concern is that often things pile up and it takes too long to get approval and the notification letter ends up sitting on an administrator's desk."

Also consider offering affected individuals free credit monitoring for a specified time to help reduce the effect of the identity theft.

"You want to do everything you can to protect yourself and your patients," says Blustein. "By monitoring

credit and notifying the right people, you might be able to cut off the use of their personal information before any damage is done."

Learning your lessons

The nature of the breach will help determine whether you want to amend your existing policies to be better prepared, educate staff members with respect to prevention, or implement more safeguards, says Blustein. Shore up any documentation pertaining to the incident in case there is an investigation, he says.

Even if you don't experience a security incident, monitor businesses and healthcare organizations in your area that may have been affected, advises Mebane.

"You can't just roll out policies and be done with it," says Blustein. "The challenges are always changing, and you need to be able to keep up with them."

Ensuring uniformity throughout your organization is important. "An organization should strive to ensure that your clinic down the street should have the same policies and protection as the computer in your main lobby," says Blustein. ■

HICI 2009 index

Breach notification requirements

Breach notification requirements: Steps facilities must take, according to federal law. July, p. 3.

Develop effective strategies for your breach notification response program. Dec., p. 1.

FTC, HHS move forward with PHR breach notification guidelines. July, p. 1.

HHS unveils online breach notification forms; experts say they're 'straightforward,' user-friendly. Dec., p. 6.

HIPAA harm threshold: Covered entities off the hook for some breaches. Nov., p. 1.

Major privacy breaches: How to respond to their unique challenges with notifying patients, government. July, p. 6.

Business associates

BA agreements: Consider additions to new contracts. June, p. 4.

BA agreements: Prevent problems and eliminate loopholes. Jan., p. 4.

Case study

Create a culture of HIPAA compliance: Hawaii facility personalizes education and eliminates problems from the start. Aug., p. 1.

Minnesota health system trains staff and tracks participation success via an online system. Aug., p. 7.

EHRs

Demonstrate differences in EHRs and PHRs. Oct., p. 1.

> *continued on p. 8*

HICI 2009 index

< continued from p. 7

EHRs, incentives on the horizon. Oct., p. 5.
Hospitals far from having fully implemented EHRs.
June, p. 6.
Update: Economy slowing growth of electronic health
record implementation in hospitals. Nov., p. 7.

HITECH Act

The HITECH Act and your organization. May, p. 1.

Medical identity theft

FTC moves Red Flags Rule compliance deadline to
August 1. July, p. 4.
FTC: 26 red flags for organizations. April, p. 4.
Include 'Red Flags' requirements in any new BA agreement.
June, p. 5.
Mark it down: Red Flags Rules deadline is May 1. April, p. 1.
Protect your organization's wallet: Comply with PCI DSS.
Feb., p. 6.

Miscellaneous

Experts: Expect more enforcement as OCR role expands.
Oct., p. 3.
Experts: HIE guidance just a framework for successful
compliance. April, p. 6.
Get administration, board members to support your
compliance program. March, p. 1.
OCR complaints: Simple steps to smooth resolutions.
Jan., p. 6.
Review and update your privacy and security incident
response policy. Sept., p. 5.
2009 HIPAA forecast. Jan., p. 1.

Privacy

AAHC: Academic health centers, researchers' time
hamstrung by privacy rule. Sept., p. 3.
AAHC: HIPAA Privacy Rule has significant effect on
research administration, processes. Aug., p. 4.
AAHC: Privacy Rule an obstacle course for biomedical
research. June, p. 1.
AAHC: Privacy Rule directly affects multisite research,
subject participation. Nov., p. 4.
Consider privacy education for patients. May, p. 6.
Employees snoop for different reasons. Dec., p. 5.
Healthcare operations: How to approach the privacy
rule's ambiguity. March, p. 3.
Limit your risk; address snooping problems swiftly,
harshly. Dec., p. 4.
Money, money, money: Privacy breaches get costly.
Sept., p. 1.
PHRs: New consumer-driven trend can lead to
better care, but also to privacy challenges.
March, p. 5.

Security

Address data encryption in 2009. Feb., p. 4.

Training

HICI survey: Most privacy and security officers will
revisit HIPAA training program. May, p. 4.
Physician offices: Tackle a different set of privacy
training challenges. Feb., p. 1.
Training topics: Explore these areas in your office
education. Feb., p. 3. ■

Relocating? Taking a new job?



If you're relocating or taking a new
job and would like to continue receiving
HICI, you are eligible for a free trial
subscription. Contact customer service
with your moving information at 800/650-6787.

Questions? Comments? Ideas?

Contact Associate Editor
Dom Nicastro
Telephone 781/639-1872, Ext. 3413
E-mail dnicastro@hcpro.com