Good cop, better cop

HIPAA privacy enforcement begins with learning, lenience

By Neil Versel

The early fear that, come April, overzealous federal HIPAA enforcers would start hauling loose-lipped doctors off to jail is now the stuff of urban legend. So says the high sheriff of the HIPAA privacy posse, Richard Campanelli, director of the HHS Office of Civil Rights.

"OCR's goal is not to maximize enforcement," says Campanelli. "Our goal is to protect personal health information. Voluntary compliance is the most effective way to do this."

And yet, the April 14, 2003, start date for HIPAA privacy rules is real and, finally, upon us.

Nearly seven years after President Clinton signed the Health Insurance Portability and Accountability Act into law—and after the government had received and processed 50,000 public comments on a 1998 regulatory proposal—physician practices and other healthcare organizations must comply with the first set of administrative regulations on the privacy of personally identifiable health information.

Unlike the HIPAA rules for electronic transactions and code sets, there will be no extension of the compliance deadline.

There is no exception for small physician practices, even though small health plans have an extra year, per the original legislation.

But take heart. Civil monetary penalties, which run as high as $100 per violation and $25,000 per year, do not apply if a nonwillful violation is corrected within 30 days, a period the OCR may extend.

In other words, the Office of Civil Rights will not be going out of its way to hunt down and penalize healthcare organizations that violate the privacy rules.

Resolve complaints quickly, informally

"I'm particularly heartened by the fact that the Office of Civil Rights is treating this as a learning and training phase rather than having the jackboots come down," says John Lumpkin, M.D., chair of the National Committee on Vital and Health Statistics, the HHS advisory board that must report to Congress annually on HIPAA effectiveness.

HHS maintains its stance that HIPAA privacy enforcement will be driven by complaints and that "most complaints can be resolved quickly, easily and informally," Campanelli says.

The department already has posted a sample complaint form on its Web site.

However, Campanelli says it is "a good idea" for covered entities to recommend that patients first file complaints with them about a privacy breach before going to the government.

There is no deadline for a covered entity to respond to a complaint, nor may individuals sue healthcare organizations under HIPAA.

"If you receive a complaint, the best thing you can do is to resolve it yourself because if you don't, the only place they can complain to is us," Campanelli tells healthcare providers.

'The Office of Civil Rights is treating this as a learning and training phase rather than having the jackboots come down.'

John Lumpkin, M.D.

Use common sense

Campanelli and other HHS officials attempted to allay the fears of the healthcare community at four public forums in February and March.

The last was a March 2 gathering in Rosemont, Ill., that drew 1,160 representatives of providers, payers, clearinghouses and technology vendors of all sizes.

Campanelli said at that meeting that the regulations, as modified in August are flexible, scalable, workable and balanced and that, within the provider community, common sense ought to prevail.

"You don't need to have a hermetically sealed room to store files," Campanelli said to the group.

There is no mandated format for the privacy notice each healthcare provider and insurer must give patients, according to David Mayer, an OCR veteran now dedicated to HIPAA privacy rule development and implementation.

Comply with me

Upcoming HIPAA deadlines

2003

April 14: Privacy compliance deadline for most entities

April 16: Deadline to begin testing transactions

April 21: Security rule effective date

Oct. 16: Transactions and code sets compliance deadline*

2004

April 14: Privacy compliance deadline for small health plans

July 30: Employer identifier adoption deadline for most entities

2005

April 21: Security compliance deadline for most entities

Aug. 1: Employer identifier adoption deadline for small health plans

2006

April 21: Security compliance deadline for small health plans

* for entities that requested an extension prior to Oct. 16, 2002

Source: CMS

Likewise, says OCR privacy program policy specialist Christina Heide, the rule calls on covered entities to put in place "appropriate" safeguards to protect information but does not prescribe how. In the case of a known violation, she says, OCR will ask the healthcare entity to mitigate the effect of an improper use or disclosure.

While this approach does allow for flexibility, it also has caused a great deal of head-scratching among covered entities.

By mid-January, only 9% of healthcare providers had completed their privacy remediation efforts, according to the most recent quarterly survey from Phoenix Health Systems, a Montgomery Village, Md.-based research firm, and the Healthcare Information and Management Systems Society, based in Chicago.

But the survey, issued in February, also reported that 75% of providers said that they will be ready by April 14.

Anecdotal evidence suggests that small and rural medical practices are the farthest behind.

"That's continuing to be a problem," says Lumpkin, who also is director of the Illinois Department of Public Health.

Still not hip to HIPAA

So, too, is ignorance of HIPAA.

Even at this late date, Patrick Padgett, staff counsel for the Kentucky Medical Association, says he gets inquiries from practices wondering if they are even subject to privacy rule.

'It looks like we are going to make it.'

David Howes, M.D.

Physician practices are exempt only if they employ fewer than 10 people and are completely paper-based, including handling of claims submissions.

And although HIPAA allows medical organizations to disclose personal health information to government officials for public policy reasons, Padgett says the Kentucky Department for Public Health has reported difficulty even in advance of the compliance deadline in obtaining information from healthcare providers.

"The KMA has been meeting with various state agencies to make them aware of HIPAA and let them know when information can be released," Padgett says.

The KMA is an active participant in the HIPAA Action Workgroup for Kentucky, or HAWK, a year-old organization that includes nearly 120 healthcare providers, payers, vendors and state agencies that help each other with HIPAA compliance efforts.

"We've done a number of seminars around the state, and we've put a number of documents and forms on our Web site,"

Know your limits

The August 2002 modifications to the privacy rule allow for use and disclosure of a "limited data set" without patient consent for research, public health and healthcare operations. A limited data set must have the following identifiers removed:

- Name
- Postal address (other than city, state and ZIP code)
- Telephone and fax numbers
- E-mail address
- Social Security number
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Internet URLs and IP addresses
- Full face photos and "comparable images"
- Medical record numbers
- Health plan beneficiary numbers and other account numbers
- Device identifiers and serial numbers
- Biometric identifiers, including finger and voice prints.

Source: HHS

Expected completion of HIPAA privacy remediation
(Survey taken in early January 2003)

	Providers	Payers	Vendors	Clearinghouses
Completed	9%	6%	20%	14%
By April 2003	75	83	51	71
Later/not sure	16	11	29	15

Source: Phoenix Health Systems, Healthcare Information and Management Systems Society

Padgett says. "We're trying to make everybody even outside of the medical community aware so, come April 14, we don't disrupt the flow of information."

Martin's Point Health Care, a 30-physician multispecialty practice based in South Portland, Maine, will finish "just in time, with a little bit of cushion," says information services director Greg McCarthy.

"I have to admit we thought that we were not going to come across the line in time, but now it looks like we are going to make it," says Martin's Point CEO and President David Howes, M.D.

The organization, which has four clinics in Maine and New Hampshire, as well as a laboratory operation, pharmacy and health plan, completed its gap analysis last summer but only began training its nonclinical employees on HIPAA privacy procedures on March 7.

"The biggest part was the gap analysis," Howes says.

Changing course midstream

The HIPAA team at Martin's Point and hundreds of thousands of other healthcare entities also had to stop in midstream and adjust to a series of modifications and clarifications HHS published in August 2002—though the healthcare community generally has accepted the changes as positive.

The rule, as modified, permits healthcare organizations to offer a "layered notice" of privacy policies so they can summarize their guidelines in a few paragraphs or bullet points.

This does not replace the requirement that all patients receive a detailed notice along with the summary.

However, there is no mandated format for the notice, so each covered entity is on its own.

"It represents a new risk-management arena," Howes says.

The August modifications also defined a

Circle this date: April 16

THERE IS NO REST for the IT-savvy physician leader.

Just two days after the April 14 privacy compliance deadline comes another critical date on the HIPAA calendar—one that has received relatively scant attention.

Healthcare entities that send and receive electronic claims data must begin testing their data transmission systems for compliance with the HIPAA rule governing transactions and code sets. Or so the law says.

Whether they will test them or not is another story.

In a survey taken during the first two weeks of January, just 43% of healthcare provider organizations said they would be ready to begin testing by the April 16 start date. An equal number said they would not be ready for seven to 10 months—leaving a razor-thin margin for error to meet the Oct. 16 compliance deadline, according to a quarterly poll by the Healthcare Information and Management Systems Society and Montgomery Village, Md.-based consulting firm Phoenix Health Systems.

But the hammer of government is not going to come down on those late with testing, according to the government. CMS, the agency charged with enforcement of the transaction portion of HIPAA administrative simplification regulations, is pushing "voluntary" compliance and conducting enforcement based on individual complaints.

At a March meeting of the Workgroup for Electronic Data Interchange-Strategic National Implementation Process, just outside Chicago, Lori Davis of the CMS Office of HIPAA Standards made it clear that CMS will not "shoot first and ask questions later."

Still, it is up to healthcare providers to make sure their transactions are in order, since software vendors have no legal responsibility to meet the HIPAA requirements.

"Just because an 835 (transaction for remittance advice) is accepted doesn't mean it's correct," says Jim Whicker, director of electronic data interchange in the accounts receivable division of Intermountain Health Care, Salt Lake City. Whicker tells of one Intermountain test of an engine meant to translate old codes into HIPAA-compliant form that created a claim based on a diagnosis that was "inconsistent with the patient's gender."

Skip McKinstry, Oklahoma City-based vice president for marketing and sales at Claredi, a transaction technology certification service in Kaysville, Utah, offers this bit of caution: "The fact that the vendor is certified does not mean that the provider is off the hook."

—N.V.

The rest of the story

AS VOLUMINOUS AS the HIPAA privacy rule is—368 pages of small type in the Federal Register, plus 92 more pages for the August 2002 modifications—some things still were left out.

For one thing, HHS does not define what constitutes a medical record anywhere in the HIPAA administrative simplification regulations.

Instead, individual organizations may determine their own core components of medical records. However, they must document the core record set and keep written and electronic copies of the documentation for six years, according to Richard Campanelli, director of the HHS Office of Civil Rights, which is responsible for enforcing civil provisions of the privacy rule.

Still, Campanelli says OCR will not review the documentation, even for enforcement purposes.

IPAs and clinically integrated care settings such as hospitals with medical staffs of independent physicians—called "organized healthcare arrangements" (OHCAs) under HIPAA—may decide whether to allow each entity within the loose affiliation to decide to have individual privacy notices and business associate agreements or if they should work together. Either way, each unit under the OHCA umbrella is separately subject to enforcement liability, Campanelli says.

Enforcement itself, HHS says, will be driven by complaints and not by random audits of privacy practices. And even though OCR has published a "sample" form for reporting perceived HIPAA privacy violations, the rule does not prescribe what a complaint should include.

"The sample complaint form on the OCR Web site is just that," says OCR official David Mayer. "It is not a mandate."

Likewise, HHS is somewhat ambiguous about the privacy notice that covered healthcare entities must present to patients, and practices have responded differently.

The notice from Carle Clinic Association, Urbana, Ill., which has about 300 physicians, comes in at about 11 pages. Meanwhile, Martin's Point Health Care, a 30-physician practice in South Portland, Maine, has a seven-page document.

—N.V.

"limited data set" (see box, page 19) of protected health information that can be disclosed without patient permission for the purpose of research, public health or healthcare operations. Healthcare organizations do not have to account for such disclosures.

In addition, covered entities can use individual records for treatment, payment and healthcare operations.

"The privacy rule is not intended to impede treatment," Heide says.

Terms of payment

Payment, according Heide, includes authorization, eligibility and benefits checking and claims adjudication. Also, Heide says, health plans may disclose personal data to reinsurance companies and stop-loss insurers as part of the payment process.

If a patient is incapacitated, the facility can use its own judgment of whether disclosure of name, location and condition to family and religious affiliation to hospital clergy is in the individual's best interest.

Likewise, pharmacists can make their own decisions on whether to allow friends or family members to pick up prescriptions for someone else.

"I think the August changes made a big difference, putting treatment on its own island," says Martin's Point project manager Kimberly Fallona. ■

HIPAA-CS
HIPAA Compliance Services

By Physicians for Physicians

- Role-based HIPAA training
- Available on CD, your intranet or website
- Designed for physician offices
- $50 per physician and their staff
- Group discounts
- Uses the case study method
- Training for each type of physician
- Office manager, office nurse, lab tech, etc.
- 31 policies written especially for offices
- 32 office forms and patient letters
- Training can easily be printed out
- Easily customized for no extra cost
- Category 1 CME available for $5/hr

Software demo: www.hipaacs.com/demo
Call Keith Van de Castle, M.D., M.B.A., M.P.H.
(434) 823-9589, keith@hipaacs.com