

- 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](mailto:dnicastro@hcpro.com)**