

- Home
- News ▶
- Technology ▶
- Markets ▶
- Personal Journal ▶
- Opinion ▶
- Leisure/Weekend ▶
- The Print Edition**
- Today's Edition
- Past Editions
- Features**
- Portfolio
- Columnists
- In-Depth Reports
- Discussions
- Company Research
- Markets Data Center
- Video Center
- Site Map
- Corrections
- My Online Journal**
- Personalize My News
- E-Mail Setup
- My Account/Billing
- RSS Feeds
- Customer Service**
- The Online Journal
- The Print Edition
- Contact Us
- Help



**HEALTH**

# Doctors, Hospitals Act To Safeguard Medical Data

**Today is Federal Deadline For Stepped-Up Security; Compliance Costs Are High**

By **CHRISTOPHER CONKEY**  
Staff Reporter of THE WALL STREET JOURNAL  
*April 21, 2005; Page D2*

On April 1, employees entering the headquarters of Blue Cross Blue Shield of North Carolina were handed fortune cookies with a message inside: "Do the right thing: support security."

The cookies were part of a campaign taking place across the health-care landscape to beef up security for confidential health information. By today, doctors, hospitals, insurance companies and others are supposed to be in compliance with a new federal rule that requires each organization to have an information security chief, a new analysis of security risks, safeguards to address vulnerabilities and training for employees on how to comply.

The question for consumers is whether the new rules will increase the chances that their private information is kept out of the wrong hands.

The security rule is the latest in a series of regulations designed to safeguard medical information and mandated by the 1996 Health Insurance Portability and Accountability Act, known as **HIPAA**. The first rule, which took effect in 2002, nudged providers and payers to use the same format in submitting and processing electronic claims. The second, which centered on privacy and went into effect in 2003, imposed limits on who is permitted to get medical information about an individual and made it easier for patients to get their own records and request changes if they thought there were errors.

The new security rule deals with the electronic, administrative and physical security of medical information. It requires health-care entities to meet

EMAIL PRINT MOST POPULAR

**▶ ALSO ON HEALTH**

- May 13
- [R.J. Reynolds Faces Suit Over Ad Claims](#)
- May 12
- [Gauging Risks of Sudden Heart Death](#)
- [MORE](#)

advertisement

**▶ E-MAIL SIGN-UP**

Don't miss the latest health news and analysis. Sign up to receive our daily newsletter. Check the box, then click below to subscribe.

**The Health Edition**

To view all or change any of your e-mail settings, [click to the E-Mail Setup Center](#)

**COMPANIES**

Dow Jones, Reuters

[Choicepoint Inc. \(CPS\)](#)

PRICE	37.73
CHANGE	-0.37
U.S. dollars	4:04 p.m.

\* At Market Close

**RELATED INDUSTRIES**

- [Health](#)

[Personalized Home Page Setup](#)

13 standards on issues including how to dispose of old records and how to respond to a security breach.

Put headlines on your homepage about the companies, industries and topics that interest you most.

Get Wall Street Journal Online NEWS ALERTS on the AOL® Instant Messenger™ Service.

SCREEN NAME: WSJ



Compliance costs for the three **HIPAA** rules are substantial. The American Hospital Association, which represents 4,700 hospitals, says hospitals will spend \$22 billion over five years complying with the 2003 privacy rule. Kaiser Permanente, the country's largest nonprofit health-care organization, expects to spend \$20 million to comply with the new security rule, including replacing 13% of its 600 software programs. By year end, says Mary Henderson, Kaiser's **HIPAA** compliance chief, the organization will have spent \$100 million on **HIPAA** changes.

Blue Cross Blue Shield of North Carolina, which says it has spent "tens of millions" complying with **HIPAA**, has required workers to adopt individualized security plans and awarded them iPods as prizes in security-related games of Jeopardy during lunch breaks.

"There's a significant weight on anyone in this business now, says Harry Reynolds, a vice president with Blue Cross Blue Shield. "The last thing you want to be is the first lawsuit."

Violations of the rule can result in criminal penalties of \$250,000 and 10 years in jail. The Department of Health and Human Services, however, hasn't been aggressively looking for lapses; instead, it's following up complaints. That enforcement stance reflects the fact that the regulations give the providers and insurers some latitude on how to comply. The new security rule says it's "impossible to dictate a specific solution" for each of the 2.6 million providers and health plans affected.

Some physicians and doctors are dragging their feet. Tom Walsh, a consultant on **HIPAA** compliance, says, "I've actually had physicians tell me, 'Who do I write the check to? I'm not interested in being compliant.'" Gary Carneal, president and chief executive of URAC, an independent accrediting body for the health-care industry, says "a lot of companies are addressing this in an ad-hoc fashion," with only a "small minority" of the 500 companies in a URAC survey in compliance.

Similarly, a study released this year by the Healthcare Information Management and Systems Society and Phoenix Health Systems found that only 18% of providers were in compliance.

Karen Trudel, deputy director of the **HIPAA** standards office at HHS, says an organization that fails to comply risks a security breach-and a badly tarnished reputation. "Would you really want to use a health-care provider if you thought they weren't safeguarding your personal information?" she says.

Advertiser Links

Featured Sponsor

Accenture Presents: "High Performance" A special advertising section [Click Here ...](#)

Investor Resource Center

FedEx Presents: "Small Business Center"

Questions for the Future: Issues that will Shape Our Future

Get IBM's On Demand Business e-newsletter

30 free trades at

In March, two laptops containing sensitive medical records for 185,000 current and former patients were stolen from the San Jose Medical Group. Also this year, the University of Chicago Hospitals reported that a former employee had stolen information on as many as 85 patients. In Florida, an employee at the Palm Beach County Health Department mistakenly sent out the names of AIDS patients.

Not all of the incidents would have been prevented by the new security rule. And even companies with vigorous security programs can't prevent some breaches, particularly those that occur from the inside. In 2003, for example, a New Jersey nurse helped identity thieves get information about terminally ill patients.

The incidents have consumers on edge. A recent survey conducted by Privacy and American Business, a nonpartisan think tank in Hackensack, N.J., found that 70% of Americans are worried that their personal information could be disclosed as a result of weak security. Moreover, concerns over the security of health records are coinciding with a wave of privacy lapses at banks, retailers and data warehouses like [ChoicePoint](#) Inc. and [LexisNexis](#) that have compromised the personal information of more than 600,000.

Mark Rothstein, a member of the National Committee on Vital and Health Statistics, an HHS advisory group, says security concerns could become so paramount for consumers that health institutions might one day have to post their security performance records, much as airlines report on-time departure rates. "I don't see any way you can make an absolutely, totally foolproof system," Mr. Rothstein says. "But we ought to

- Ameritrade.
- Accenture Presents:  
"High Performance"
- Financial HP  
Workstations at PC  
Prices

keep trying."

**Write to Christopher Conkey** at [christopher.conkey@wsj.com](mailto:christopher.conkey@wsj.com)

 [EMAIL THIS](#)  [FORMAT FOR PRINTING](#)  [MOST POPULAR](#)  [ORDER REPRINTS](#)

Sponsored by



[Return To Top](#)

---

[Log Out](#) [Contact Us](#) [Help](#) [E-Mail Setup](#) [My Account/Billing](#) [Customer Service: Online](#) | [Print](#)  
[Privacy Policy](#) [Subscriber Agreement](#) [Mobile Devices](#) [RSS Feeds](#) [News Licensing](#) [About Dow Jones](#)

Copyright © 2005 Dow Jones & Company, Inc. All Rights Reserved



