

*Along with the new federal stimulus bill comes new HIPAA enforcement provisions and other requirements for healthcare providers. To help our D.C.s with this issue, we asked our HIPAA partner, HIPAA Solutions Rx, to outline some of the changes.*



# What You Need to Know about **HIPAA Changes**

By Peter N. Cizik, HiPAA Solutions Rx

**If you've been monitoring the activity in Washington, you're probably aware that the stimulus bill includes a number of provisions. These include several affecting HIPAA Privacy and Security regulations, such as:**

- **New Enforcement Rules** — Audits will be proactively performed and state attorney generals can prosecute criminal violations. Fines have been raised.
- **Business Associates and Covered Entities** — Business associates now have as much responsibility to safeguard protected health information (PHI) as the covered entities themselves. Business associates are non-staffers who have access to a covered entity's PHI. For D.C.s this may mean labs, billing companies and more.
- **Increased Liability** — Individuals, as well as organizations, can be held accountable for violations.
- **Restrictions on Information Disclosures** — Individuals can

request procedures not be disclosed to health insurers if they pay for procedures out of their own pockets.

- **New Disclosure Rules** — In the event of a large breach, offenders will be required to post announcements in newspapers and alert certain authorities, as well as those directly impacted by the breach.

As with any regulation, the devil is in the details, and you should be cautious about making broad assumptions about any provision. Here are just a few things D.C.s who own small practices should do:

## **1. Tighten up information security.**

There are new actions required for breaches of "unsecured" PHI. Encrypt data whenever you can — particularly on any laptops — and don't email PHI unless it's encrypted. To find out more about securing data on your laptops, conduct a web search on "file encryption system" or

"disk encryption systems." MS Windows has a built-in capability, but it requires some technical know-how to set up and use. A third party application may be a better option.

If you email PHI, either use a web-based secure email provider to exchange confidential information (e.g. Postini) or purchase software that integrates with your email program (e.g. PGP, Verisign Digital IDs) that can automatically encrypt the message and any attachments before they are sent (since it requires the receiver to have similar software, it's not a good option for people you email infrequently) or have a secure area on your own website where users can create a username/password and send you secure messages that way. There are many providers of these various products and services, so talk with a technology support person for recommendations.

## **2. Make sure your business associates have agreements in place.**

---

If you think your HIPAA program needs updating, go to [www.ncmic.com](http://www.ncmic.com) and click on the "HIPAA Training" link under "Resources for D.C.s" for information on HIPAA Solutions Rx training, as well as the discount to NCMIC policyholders. Current participants can order a supplement to the HIPAA manual that includes the latest changes.

It's a legal responsibility of both parties now. Ensure they report any breaches to you, and make sure you log and report these annually.

### 3. Train yourself and your staff on the latest information and stay abreast of changes.

For more in-depth information and to download a comprehensive overview of the provisions, go to [www.bridgefront.com/solutions\\_education\\_hipaa\\_stimulus.php](http://www.bridgefront.com/solutions_education_hipaa_stimulus.php). You can also sign up for *HIPAA Flash*, HIPAA-Rx's free newsletter. ◀◀

*Peter Cizik is the chief executive officer and co-founder of BridgeFront and HIPAA Solutions Rx (now a subsidiary of BridgeFront). HIPAA Solutions Rx has become the premier provider of HIPAA compliance products and services to the healthcare industry. Mr. Cizik has co-authored several articles on complying with the HIPAA regulation and has done numerous presentations on the topic to groups and associations around the country. A graduate of the Harvard Business School, Mr. Cizik has spent more than 20 years in a variety of operating and senior management roles in small startups and Fortune 500 companies.*

## Real-world Privacy and HIPAA Cases

**Richard Gibson admitted he had disclosed a patient's PHI** to obtain credit cards in the patient's name. Gibson then used the credit cards to make thousands of dollars worth of personal purchases. He was convicted and sentenced to 16 months in prison in November 2004 and had to make restitution to the credit card companies and the identity theft victim.

**Andrea Smith was convicted of accessing and disclosing a patient's health information** from her place of employment in December 2008. She was sentenced to two years probation and 100 hours community service.

**Isis Machado passed on PHI of more than 1,100 Cleveland Clinic Hospital patients** to her cousin who owned a claims service company. The cousin then filed over \$2.5 million in fraudulent Medicare claims. Machado pled guilty to conspiracy and received three years probation in exchange for testimony against her cousin. The cousin was found guilty and sentenced to over seven years. Both were ordered to pay \$2.5 million each in restitution.

**Providence Health & Services was assessed a \$100,000 HIPAA fine** after failing to properly secure data backup tapes, disks and laptops. During 2005 and 2006, medical data was stolen or lost when laptops transporting patient data were taken outside of the health system's buildings.

**CVS Caremark paid \$2.5 million to settle allegations** of HIPAA privacy rule violations in February 2009. The Department of Health and Human Services (HHS) began the investigation after media reports of patient information being disposed of in unsecured industrial trash containers outside the CVS stores. CVS is now required to hire a third party to assess their compliance and report to the HHS and the Federal Trade Commission (FTC). The FTC is also investigating whether CVS failed to protect the sensitive financial information of its customers. CVS will be monitored by the HHS for three years and the FTC for 20 years.

NCMIC INSURANCE COMPANY

# Seminars

With our policy, full-time D.C.s get a

## 5% DISCOUNT

for three consecutive policy years\*

#### November 21

Casper, Wyoming

Co-Sponsor: Wyoming Chiropractic Association

Speaker: Stephen Perle, D.C., MS

Topic: Rehabilitation (8 hours)

To register: Contact Lisa Popp at 307-315-2265

#### November 21

Richmond, Virginia

Co-Sponsor: Virginia Chiropractic Association

Speaker: Stephen M. Savoie, D.C., FACO

Topic: Documentation (8 hours)

To register: Contact VCA at 540-932-3101

#### December 5-6, 2009

Levittown, New York

Co-Sponsor: New York Chiropractic College

Speaker: Anna K. Allen, RN, MSN, CLNC

Topic: Ethics (3 hours)

Speaker: Stephen M. Savoie, D.C., FACO

Topic: Risk Management (10 hours)

To register: Contact NYCC at 516-796-5923

#### December 5-6, 2009

Nashville, Tennessee

Co-Sponsor: Tennessee Chiropractic Association

Speaker: Scott D. Banks, D.C.

Topic: Sacroiliac Dysfunction and Pelvic Pain Spectrum (8 hours)

Speaker: Steven J. Gould, D.C., D.A.C.B.R.

Topic: Radiology (4 hours)

To register: Contact TCA at 615-383-6231

Go to the Continuing Education section of [www.ncmic.com](http://www.ncmic.com) for additional listings.

\*Seminar discounts earned up to 30 days after the policy renewal date will apply immediately; those earned 30+ days after the renewal date will apply at the next policy renewal date. Discounts apply to NCMIC malpractice insurance by attending a qualifying seminar of at least eight hours.