troinet

troinet.com

Why the HIPAA Police Woke Up, New Rules & 5 Things You Can Do To Protect Your Practice

Why the HIPAA Police Woke Up, New Rules & 5 Things You Can Do To Protect Your Practice

HIPAA has not been aggressively enforced for years, but at the same time there have been sweeping changes to the rules that have been in effect since 2005. With the change from film to digital images, and new high-tech dentistry tools, combined with changes to HIPAA affecting patients' rights and your vendors, you can't afford to sit back. The 'HIPAA Police' woke up when risks became higher than ever before.

The 'HIPAA Police'

The HITECH Act of 2009 funded $36 billion for Electronic Health Records systems for doctors and hospitals. Enforcement of HIPAA was instantly multiplied by 50 when the state attorney generals were given authority. Business Associates and their subcontractors (now including data centers, paper storage facilities, and Cloud services) have to comply with HIPAA, and are directly liable for data breaches they cause.

After HIPAA enforcement was funded and the enforcement agency was told they could keep the penalties they collect, the first thing they did with their funding was hire a former federal prosecutor to run the agency. He has gone after small practices, hospitals, government agencies, and a small hospice.

Fines included $1.5 million for a lost laptop, $1.7 million for a lost backup drive, $100,000 for using Gmail to send patient records, and $400,000 for a failed network firewall. The enforcement agency's 2013 budget was $38 million and they collected an additional $4 million this year in fines.

What's New

The changes to HIPAA came out in January 2013, modifying the original Privacy and Security Rules. These changes required that Notices of Privacy Practices and Business Associate Agreements be updated. The data breach laws were changed to increase risks of a large penalty if an unencrypted laptop or other portable device that contains patient data was lost.

5 Things You Need To Do

1. **Give a New Notice of Privacy Practices (NPP) to New Patients.** You don't have to send new ones to your existing patients, but you must post a new version and make them easily available in your waiting area.

2. Gain Control of Your Business Associates. Each vendor that has access to any patient data must sign a Business Associate Agreement containing new wording that was released in January. Each Business Associate had to comply by September 23, 2013 and ensure than any subcontractors they work with are also compliant. The new rule requires that paper storage companies, data centers, online backup providers, and Cloud service providers comply as Business Associates even if they never look at your patient data. You must replace your current agreements by September 2014.

3. Have a Competent Technical Company Review the Security of Your Workstations and Your Network. Computers that have consumer-level operating systems cannot protect patient data. Network devices must be tested to ensure that security is working (the last HIPAA penalty was $400,000 for a firewall that failed silently and allowed 17,000 patient records to be breached). A burglary of four computers in a doctor's office resulted in the breach of 4 million patient records including Social Security numbers. An executive said the data should have been stored on more secure systems. Have your network checked for security vulnerabilities and have them fixed, if needed. Work with a competent IT company to provide Managed Services to ensure you remain secure.

4. Train Your Entire Staff. Most data breaches are caused by people who don't know what to do. HIPAA requires training - your managers need to understand the rules, how to

prevent data breaches, and what to do if one occurs. Your workforce needs to know proper behavior—what they should and shouldn't do to minimize the risk that patient data will be lost or accessed by an unauthorized person.

5. **Stop Bad Habits.** Never send patient data (words, voice files, or images) to anyone using web mail (Gmail, Yahoo!, MSN, etc.) Never send patient information by text message. Voice messages are as protected as the written word. Make sure your users each have a unique login and password, and that your computers automatically log off. Security can be inconvenient, but the benefits are worth it.

Contact PACT-ONE to discuss how we can help you build HIPAA-compliant policies and procedures, train your managers and workforce, and provide ongoing technical services to protect data and avoid fines.

1200 South Avenue
New York, NY 10314
Phone: 718-761-2780
Fax: 718-761-2784