HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc. September 19, 2015 Volume 1, Issue 9

Serving the Roanoke area since 2006

HIPAA Audits About To Increase

September 2015

The HHS Office for Civil Rights (OCR) announced that Deven McGraw will join the OCR team as the Deputy Director for Health Information Privacy effective June 29, 2015.

McGraw will spearhead OCR's policy, enforcement, and outreach efforts on the HIPAA Privacy, Security, and Breach Notification Rules; as well as lead OCR's work on Presidential and Departmental priorities on health privacy and security.

The next phase of audits will begin after OCR submits information about its plans for public comment late this year or early in 2016, she said in an exclusive interview with Information Security Media Group.

McGraw also said that "…carelessness is often a key factor…" in data breaches and that "…reasonable safeguards…" should be taken by medical practices to protect ePHI. She went on to say "…**to send a message to folks that we are quite serious about audits and we are going to continue to use that tool**…"

She further said that **performing a Security Risk Analysis** is the most important thing a Medical Practice can do. **«**

COMPUTER NETWORKS, INC
www.computernetworksinc.com
OF ROANOKE

WHY DO I NEED A SECURITY RISK ANALYSIS?

CANCER CARE GROUP PAYS $750,000

SEPTEMBER 2, 2015

$750,000 HIPAA SETTLEMENT EMPHASIZES THE IMPORTANCE OF RISK ANALYSIS AND DEVICE AND MEDIA CONTROL POLICIES

Cancer Care Group, P.C. agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules with the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR). Cancer Care paid $750,000 and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Cancer Care Group is a radiation oncology private physician practice, with 13 radiation oncologists serving hospitals and clinics throughout Indiana.

On August 29, 2012, OCR received notification from Cancer Care regarding a breach of unsecured electronic protected health information (ePHI) after a laptop bag was stolen from an employee's car. The bag contained the employee's computer and **unencrypted backup media**, which contained the names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of approximately 55,000 current and former Cancer Care patients.

OCR's subsequent investigation found that, prior to the breach, Cancer Care was in widespread non-compliance with the HIPAA Security Rule. It had **not conducted an enterprise-wide risk analysis** when

HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc. September 19, 2015 Volume 1, Issue 9

Serving the Roanoke area since 2006

the breach occurred in July 2012. Further, Cancer Care **did not have in place a written policy specific to the removal of hardware and electronic media containing ePHI into and out of its facilities**, even though this was common practice within the organization.

OCR found that these two issues, in particular, contributed to the breach, as **an enterprise-wide risk analysis could have identified the removal of unencrypted backup media as an area of significant risk to Cancer Care's ePHI**, and a comprehensive device and media control policy could have provided employees with direction in regard to their responsibilities when removing devices containing ePHI from the facility.

"Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information," said OCR Director Jocelyn Samuels. "Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information." **«**

A **Security Risk Analysis** is *required* for compliance. Call us today if you have not done yours or have questions about the process.

Hank Wagner
757-333-3299 x232
hank.wagner@computernetworksinc.com

Have You Committed Medicare Fraud?

Folks, you were supposed to have conducted your first HIPAA Security Risk Analysis in 2005 to identify problems in your organization related to protecting electronic Protected Health Information (ePHI).

If you attested to Meaningful Use without having conducted a proper Security Risk Analysis, and without having remediated the problems found, you have most likely committed Medicare Fraud since you took money from CMS as part of the American Recovery and Reinvestment ACT (ARRA).

If you think that might be the case, then it is time to step up to the table and get your Practice compliant BEFORE the folks at OCR show up. **«**

NEW! 36 Month HIPAA Compliance Plan

We have a new HIPAA program!

We now offer 36 months of HIPAA compliance consulting (includes a complete onsite Security Risk Analysis, Remediation Plan, quarterly network scans for 3 years, Policy and Procedure templates, including guidance on implementing, incident investigation, breach investigation, unlimited HIPAA compliance questions) for one low monthly fee. Ask, call, or email me for details!

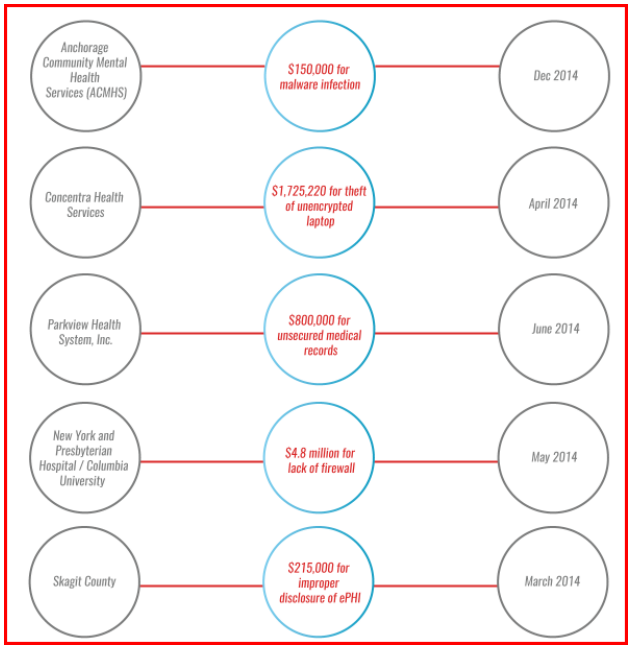
HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc. September 19, 2015 Volume 1, Issue 9

Serving the Roanoke area since 2006

Sample HIPAA Fines

If you don't think HIPAA violations can happen to you, take a quick look at these fines. Is YOUR Doctor going to be happy paying fines of this magnitude?



Wake up and smell the coffee folks…get your Security Risk Analysis done, get it documented, fix the problems that you found, then wait a few months and repeat the process. No one is immune. There is PHI in places that you do not believe you have PHI, there are staff using work-arounds that expose PHI to others, there are employees who do not understand and sometimes do not care, you have PHI on your Smartphone, at your answering service, with the transcription service…PHI is everywhere.

Find it. Protect it. **«**

Missed The Boat?

So, if you have yet to:

- Take protection of PHI seriously
- Conduct a Security Risk Analysis
- Update an existing Security Risk Analysis
- Develop a Culture of Compliance
- Look at HIPAA as a journey
- Document your compliance

You are missing the boat. The Federal Government is about to "break bad" on the medical offices that are failing or refusing to take the HIPAA process seriously.

You must develop a new way of thinking. Compliance with HIPAA is now a part of everyday life and it is not just about having a Notice of Privacy Practices for your Patients to sign every now and again.

You must have Physical, Technical and Administrative safeguards in place, you must have documentation of how you have met these safeguards and you must have an ongoing review process.

Ignoring these HIPAA rules is akin to ignoring the Internal Revenue Service. You can do it, but, when you get caught it is not going to be pretty and it is going to be very expensive.

Do not put your Physician/Owner's business in jeopardy. Talk to us about a Security Risk Analysis today and what you need to do to get and remain compliant. **«**

HIPAA SECURITY BRIEF

By Computer Networks of Roanoke, Inc. September 19, 2015 Volume 1, Issue 9

Serving the Roanoke area since 2006

Cliff Notes from the Joint OCR/NIST HIPAA Security Conference

September 2015

Risk Assessment. From the opening remarks of new OCR Director Jocelyn Samuels to the closing OCR Update presentation and almost every presentation in between, the risk assessment was highlighted as a critical compliance measure. Director Samuels pointed out that "an enterprise-wide risk assessment is the cornerstone of compliance." She also noted that OCR continues to see failures on this issue, including failure to conduct a risk assessment, incomplete risk assessments, and failure to review and update risk assessments regularly. Director Samuels stated that enforcement will be important to address these failures. Iliana L. Peters, OCR's Senior Advisor for HIPAA Compliance and Enforcement, echoed the importance of the risk assessment as a compliance measure in her presentation and highlighted the tools available through NIST, the Office of the National Coordinator, and OCR to assist in this effort, such as the Security Risk Assessment Tool.

Takeaway: There is really no excuse for not conducting a risk assessment, and those who are out of compliance should not expect sympathy from OCR.

Workforce Training. Training and education were additional compliance measures highlighted throughout the conference. Education is "the best compliance tool" according to Matthew Scholl, Acting Chief of NIST's Computer Security Division. OCR acknowledged that breaches were inevitable, but critical to any OCR enforcement decision is the existence of compliance measures and systems in place to address the inevitable breach, such as workforce training. As many of the speakers emphasized during the conference, during OCR's Pilot Audit Program, 58 out of the 59 health care providers audited had at least one negative finding regarding Security Rule compliance. Government officials who spoke at the conference indicated their belief that inadequate workforce training was a key factor in yielding these audit findings. Moreover, their presentations made it clear that the agency may take an expansive view of who is part of a covered entity's workforce.

Takeaway: No compliance program is effective if employees and contractors don't know anything about it!

Adequate Encryption. Encryption was highlighted throughout the conference as a critical security measure and an entire panel was dedicated to Safeguarding Data Using Encryption. The NIST speakers in this session pointed out that encryption cannot prevent attacks or other losses of data, but can prevent a world of problems if the data is actually compromised. OCR enforcement officials echoed this theme by pointing out that 60% of breaches reported on OCR's so-called "Wall of Shame" for data breaches affecting 500 individuals or more, resulted from theft and loss. According to OCR, encryption would have prevented all of these breaches. Further, the speakers in the encryption session made it clear that as breaches by outside actors get more and more sophisticated and medical identity theft gets increasingly lucrative, health care organizations need to ensure that the level of encryption is sufficient for their security needs.

Takeaway: Encryption is an addressable (not mandatory) security standard under HIPAA. However, in the event of a breach, investigation or audit, it will be extraordinarily difficult to convince OCR that encryption is not a reasonable security measure for your organization.

Courtesy of: Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.