HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

January 15, 2016

Volume 2, Issue 1

Security Resolutions For 2016

Rebecca Herold-The Privacy Professor

Most CEs fail to appropriately vet and oversee their BAs. Most CEs, as well as BAs, address HIPAA compliance as a checklist activity instead of a comprehensive risk management process. And many do not provide effective training or awareness communications.

"A risk assessment is an important tool in identifying risks, but you cannot stop there."

As a result, I recommend organizations make three New Year's resolutions to help bolster security and minimize the risk of a data breach:

1. **Ramp Up Contractor Scrutiny**
Do you know how well your vendors, business associates and contracted third parties - who I will collectively call "contractors" - are protecting the information with which you've entrusted them to perform some sort of business activity?

Keep in mind that about 20 percent of breaches on the HHS "wall of shame" of major health data breaches involve a BA.

Also, be aware that your organization will probably share liability for the bad actions of your contractors. Case in point: In November, the Connecticut Attorney General applied penalties against both Hartford Hospital and its business associate, EMC Corp., as a result of a breach that occurred in 2012.

In 2016 make sure your contractors:
•Have documented policies and procedures. If they aren't documented they don't exist.
•Understand that they must appropriately secure, and not share, the personal information you've entrusted to them.
•Provide regular information security and privacy training to their workers, and regularly send awareness reminders.
•Have a risk management process in place.
•Have implemented basic security tools to protect the information you've entrusted to them.

2. **Go Beyond a Risk Management Checklist**
It's vital to address administrative, technical and physical risks. Significant breaches have occurred as a result of not addressing all of these risks. Of course, a risk assessment is an important tool in identifying risks, but you cannot stop there. You need to implement a risk management program that includes additional activities to manage risks, such as keeping track of mobile computing devices with access to PHI; documenting those using personally owned computing devices; staying on top of new Internet of Things plans; making sure big data analytics is not used in a way that brings unacceptable security and privacy risks; keeping anti-malware updated and applying security patches regularly; and performing audits, just to name a few.

Here's a perfect case in point. After numerous breaches, on Nov. 30, 2015, Triple-S Management Corp. agreed to pay a $3.5 million dollar HIPAA non-compliance fine and to implement a robust corrective action plan to establish an effective HIPAA compliance program with effective security controls. Among the HHS findings:

•Failure to implement appropriate administrative, physical, and technical safeguards;
•Impermissible disclosure of PHI to an outside vendor with which it did not have an appropriate business associate agreement;
•Failure to conduct an accurate and thorough risk analysis; and
•Failure to implement security measures sufficient to reduce the risks and vulnerabilities to its PHI to a reasonable and appropriate level.

If the insurer had a comprehensive risk management program in place, including keeping systems patched and up-to-date, Triple-S probably could have prevented the breaches.

3. **Educate the Workforce**
Information security and privacy education is more important than ever because new gadgets and technologies enable more healthcare workers to collect and share data.

In September 2015, Cancer Care Group agreed to settle HIPAA violations by paying a $750,000 fine and adopting a "robust corrective action plan to correct deficiencies in its HIPAA compliance program." One of the major requirements for Cancer Care Group was to review and revise its training program, because the breach was caused by an easily preventable employee action (leaving a laptop with clear text files of 55,000 patients in an unsecured car).

Training needs to be more than once a year, and as soon as, or prior to, the start of employment. There also needs to be ongoing awareness, communications and activities, as required by HIPAA.

Every organization of every size needs to invest some time and resources into regular training and ongoing awareness communications. Besides being a wise business decision, it's also a requirement in most data protection laws and regulations to provide such education. ☸

PHI is everywhere. Find it. Protect it.

Obama Administration Changes HIPAA Rules Using Executive Order

The Department of Health and Human Services' Office for Civil Rights said it will change the rules so that mental health providers can share data with the National Instant Criminal Background Check System, part of a slate of executive actions President Barack Obama on January 5th, to help curtail gun violence.

NICS is maintained by the FBI to conduct background checks on people who may be legally disqualified from owning guns.

Specifically, the HIPAA Privacy Rule change will enable mental health providers to show the identities of patients subject to a federal mental health prohibitor that prevents them from shipping, transporting or possessing a firearm, according to OCR.

However, the new rule prohibits mental health providers from sharing any diagnostic or clinical information from medical records or other sources beyond the fact that a person is barred from gun ownership.

An NICS Index record consists of "the name of the ineligible individual; the date of birth; sex; and codes indicating the applicable prohibitor, the submitting entity, and the agency record supporting the prohibition (e.g., an order for involuntary commitment)," according to the rule. ☸

PHI is everywhere. Find it. Protect it.

Child Welfare Agency Employee Emails 970 Records to Personal Email Address

Dec 31, 2015 | HIPAA Journal

Hillsides, a child welfare agency based in Pasadena, CA, has discovered that a former employee emailed highly confidential patient and employee data to a personal

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

January 15, 2016

Volume 2, Issue 1

email address over the course of a year, in breach of Health Insurance Portability and Accountability Act Rules.

The HIPAA breach was discovered on December 8, 2015, and an investigation into the incident was immediately launched. That investigation revealed confidential data had been sent to the employee's email account on five separate occasions. The first incidence occurred on October 10, 2014. No information has been released to indicate why the information was emailed. When data is taken or emailed to personal email accounts, the individuals responsible usually do so with a view to using the information when they change employer, to sell data to identity thieves, or to personally use the information to commit fraud or identity theft.

The latter would be possible in this case as the information contained in the files attached to the emails included patient names, addresses, dates of birth, genders, Social Security numbers, medical ID numbers, and the names of the patients' therapists and rehabilitative therapists. The data of 502 patients of the welfare agency were contained in the lists.

It is not only patients that have been impacted by the HIPAA breach. Files containing the names, addresses, medical ID numbers, and Social Security numbers of 468 Hillside employees were also emailed to the employee's account.

The employee's work contract was terminated as a result of the privacy violation; however, Hillsides staff were unable to recover the data files that had been sent to the employee's personal email account. Consequently, there is a chance that the data may not have been deleted and could be used inappropriately. Hillsides has not received any reports of the data being used inappropriately at this point in time.

At the present moment in time, criminal charges against the individual have not been filed. It would also appear that credit monitoring and identity theft protection services are not being offered to affected individuals, even though Social Security numbers and dates of birth were contained in the emailed files.

Instead, affected individuals have been encouraged to contact Equifax, Experian, and Transunion and obtain free credit reports. Individuals are permitted to obtain one free credit report from each of the three credit monitoring bureaus every 12 months without charge. ☸

Just Make It All Go Away!

NEW! 36 Month HIPAA Compliance Plan

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

PHI is everywhere. Find it. Protect it.

Snooping Is Not Allowed

I am finding that some folks are unaware that looking at a Patient's medical record, without a legitimate reason to do so, is a HIPAA violation that constitutes a data breach that is reportable to the Office for Civil Rights.

You are supposed to have logging turned on in your EHR/Practice Management software and you are supposed to be regularly auditing those logs to insure that your staff is not snooping on your Patients. ☸

PHI is everywhere. Find it. Protect it.

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

January 15, 2016

Volume 2, Issue 1

Top 7 Data Breaches for 2016

The top 7 breaches:

1. Excellus BlueCross BlueShield: The Excellus BlueCross BlueShield hack was the third-largest healthcare breach of 2015, exposing personal data from more than 10 million members after the company's IT systems were breached, beginning as far back as December 2013.

2. Premera Blue Cross: Premera announced its cyberattack, affecting the data of more than 11 million members, just one month after the Anthem Blue Cross breach. The company discovered the cyberattack in January, but the initial breach occurred in May 2014. Employees of Microsoft, Starbucks and Amazon were some of the customers affected.

3. VTech: Marking the first breach to directly affect children, in November an unauthorized party obtained customer data from the Learning Lodge app store and Kid Connect servers, exposing the data of more than 6 million children and nearly 5 million parent accounts.

4. Experian/T-Mobile: Attackers breached one Experian North America business unit server, containing the personal data of about 15 million T-Mobile customers. The cause was T-Mobile sharing customer information with Experian to process credit checks or financing.

5. OPM: The personal information of more than 21.5 million citizens, including 5.6 million fingerprint records was compromised from the Federal Office of Personnel Management cyberattack, exposing 19.7 million individuals who applied for security clearances, 1.8 million relatives and other government personnel associates and 3.6 million current and former government employees.

6. Ashley Madison: The Impact Team hacker group accessed the Ashley Madison user database, revealing financial records and other proprietary information, including the personal data of 37 million users. The group's manifesto uncovered the "full delete feature" was false and personal information of its users was kept on file.

7. Anthem: In February, Anthem made history as the largest healthcare breach ever recorded. Initially, Anthem estimated approximately 78.8 million highly-sensitive patient records were breached, but that quickly increased to an additional 8.8 to 18.8 million non-patient records. Anthem's attack was just the first of many healthcare breaches of 2015; CareFirst BlueCross BlueShield and the UCLA Health Systems were also hacked. ☸

PHI is everywhere. Find it. Protect it.