October 2015 Volume 1 Issue 10

HIPAA Advisor

Because We Care, We're HIPAA Aware

HEALTH CARE SERVICES DIVISION

PRIVACY FACTS

Who is the OCR?

Becky Reeves & Trish Rugeley
Compliance & HIPAA Privacy Officers

The Department of Health and Human Services' Office for Civil Rights (OCR) is a federal agency whose mission is to improve the health and well-being of people across the United States; to ensure that people have equal access to and the opportunity to participate in and receive services from Medicare, Medicaid, and other federal programs without facing unlawful discrimination; and to protect the privacy and security of health information.

The OCR investigates complaints related to civil rights, including HIPAA. It also investigates all breaches that involve 500 or more individuals. OCR provides written guidance to providers on how to comply with HIPAA. OCR performs audits on providers to measure HIPAA compliance. And finally, OCR has the ability to levy fines against providers should they determine an unacceptable level of non-compliance with the HIPAA regulations. Those fines can be quite hefty, so it is important that we all do our part to comply with the regulations!

Phase 2 of OCR Audits are slated to begin very soon. Hospitals and Business Associates will be chosen at random to be part of the audit. The audits will be desk audits and the entity will have two weeks to respond to the OCR's information request. Your HIPAA Privacy and Security Teams are busy making sure we are ready for these audits should we be chosen!

How to Tell If You've Been Bit by the QUARANTINE Medical ID Theft Zombie

Medical identity theft is hard to detect, and many people still alarmingly do not understand that it's a real and present danger.

In the first episode of the new AMC show, "Fear the Walking Dead," it takes a while for Los Angeles to understand what's happening, i.e., that the zombie apocalypse has begun. We are in a similar situation with medical identity theft, but in the real world version, with vigilance on your part, you can better protect yourself.

Here are the telltale signs you've been infected:

- There is an error on your medical file. While this can happen in the usual way—even doctors make mistakes—it could signal trouble. TIP: Many doctors provide online access to your medical records. If yours does, take advantage of it and make sure the information there is accurate. If you cannot access your file, ask your doctor to read it to you.
- You receive phishing emails that refer to your healthcare provider or billing that require personally identifiable information to learn more. **TIP:** Always look up and call the main number of any entity that requests personally identifiable information. Only authenticate yourself when you are in control of the virtual or telephonic conversation.

More From Credit.com:

3 Dumb Things You Can Do With Email

- You get one-ring phone calls. **TIP**: If you do not recognize the number, let it go to voicemail. Some fraudsters call your phone number after purchasing your information on the black market to see if your number works (i.e., your file is worth trying to exploit). Never return a one-ring call to ascertain who called, because these can also be scams that trigger a charge on your phone bill.
- Your Explanation of Benefits lists a doctor visit you didn't make or a prescription that wasn't issued to you. **TIP**: Read all your mail from healthcare providers, making sure that there is nothing in the correspondence that could point to fraud. If you suspect your information has been used, call your healthcare provider immediately.
- You are contacted by a debt collector regarding your failure to pay in a timely manner a doctor, laboratory or medical facility. **TIP:** Demand that the debt collector provides the details within five days and immediately contact the medical provider and your insurer.

Any opinions expressed in this column are solely those of the author. Adam Levin is chairman and co-founder of Credit.com and IDT911. He is a nationally recognized expert on identity theft and credit. His new book, "SWIPED: How to Protect Yourself in a World Full of Scammers, Phishers, and Identity Thieves" will be released this fall.

SECURITY FACTS

DISASTER RECOVERY

James "Mickey" Kees

Chief Information Officer / HIPAA Security Officer

HIPAA not only protects PHI from inappropriate access, use, or disclosure. HIPAA also requires hospitals to protect PHI from being lost or distorted. Under HIPAA, Leadership and the HIPAA Security Team must have a plan to address disaster recovery of patient data in any of its electronic forms. The hospital must be able to establish, and implement as needed, procedures to restore any loss of data as well as keep that data safe in an emergency situation. And just like in any other aspect of emergency preparedness, the hospital must "practice" what would happen in an emergency situation by having a drill to test its plans and systems.

How are YOU a part of this Disaster Recovery system? Most revenue cycle departments have "downtime" procedures that are documented and used during times of outages. These are the same processes you will use in an actual disaster. Make sure that you and your department are familiar with these downtime procedures, and work on any issues with the processes' effectiveness BEFORE an actual disaster occurs. Living in southern Louisiana, we never know when the next disaster may strike. And we want to make sure that our patients' health information is accurate, safe, and secure.

FAQ FROM OCR

The Office for Civil Rights, the organization responsible for educating providers about HIPAA, has a website with Frequently Asked Questions (FAQs). Here is one such question from their website.

QUESTION: Do the Security Rule requirements for access control, such as automatic logoff, apply to employees who telecommute or have home-based offices if the employees have access to electronic PHI (e-PHI)?

ANSWER: Yes. Covered entities (like Lallie Kemp and HCSD) that allow employees to telecommute or work out of home-based offices, and have access to e-PHI, must implement appropriate safeguards to protect the organization's data….The information access management and access control standards, however, require the covered entity to implement policies and procedures for authorizing access to e-PHI and technical policies and procedures to allow access only to those persons or software programs that have been appropriately granted access rights.

POLICY HIGHLIGHT

LSU HCSD has numerous policies that help you protect our patient's PHI. To locate these policies go to the LSU HCSD website – www.lsuhospitals.org - click on Employees, then select HCSD policies.

LSU HCSD POLICY 8515 BREACH NOTIFICATION

Breach Notification, outlines the processes that LSU HCSD and Lallie Kemp Medical Center must take any time there is the possibility that a patient's protected health information may have been inappropriately accessed, disclosed, acquired, or used. The policy outlines the steps taken by the compliance and legal departments when determining whether or not an incident rises to the level of a breach. A breach is typically considered to have occurred when there is a greater than small chance that the PHI has been "compromised" and it is the responsibility of Lallie Kemp or LSU HCSD to prove that the PHI was NOT compromised in order to determine that there is not a breach.

If a breach has occurred, the policy outlines the steps that must be taken to notify the patient(s) of the incident, as well as the federal department of Health and Human Services. If the breach involves 500 or more individuals, the news media must also be notified. The notifications must occur as soon as possible, but not longer than 60 days from the time of the discovery of the breach. A breach is considered to be "discovered" when someone at Lallie Kemp or LSU HCSD becomes aware of it.

The policy is a lengthy one, due to the complexity and detail in the federal statute outlining Breach Notification. It is because of that complexity that Compliance needs to be notified immediately once a possible breach is discovered.

Volume 1 Issue 10

HIPAA TIME
Headlines That Matter to You

HIPAA Breach Hits Close to Home

The LSU Health New Orleans School of Medicine reported to news media outlets this September that the PHI of approximately 5,000 minor patients was compromised when a laptop was stolen from a member of the faculty. The physician, who is an urologist on staff at the School of Medicine reported that his laptop was stolen from his car during the night after he had left the laptop in his car. The car was parked in front of his home. The information on the pediatric patients included names, dates of birth, dates of treatment, descriptions of patients' conditions, treatments, and outcomes, lab test results, radiologic and ultrasound images, and diagnosis and treatment information.

It took the Office of Compliance at LSU Health Sciences Center New Orleans eight weeks to reconstruct the files that could have been stored on the laptop to identify any patients whose information may have been compromised. When using the laptop, the data was not saved to the LSU Health Sciences Center New Orleans servers, but, instead, to the laptop's hard drive, causing the difficulty in identifying the patients affected In addition, the laptop was not encrypted.

Lesson Learned:

LSU Health Care Services Division prohibits the storing of PHI on unencrypted laptops and other mobile devices. LSU HCSD also strongly encourages those who have encrypted laptops to still store any PHI on LSU HCSD servers (e.g., the "O" Drive) instead of their laptop. Laptops must be secured at all times. Frequent HIPAA stories in the news have shown that storage of a mobile device in a vehicle is NOT a secure method of storing such devices.

Cost of Cyber Attacks to Health Care Systems to Rise to $305 Billion

As recent news stories highlight, cyber attacks on health care payers and providers is at an all time high. A recent study performed by Accenture used data available from the Ponemon Institute and the Office for Civil Rights to determine the number of individuals who were at risk for identity theft through health care. Then Accenture quantified the patient revenue that would be put at risk as a result of a data breach. The figures were then projected for the next five years.

Over the next five years, Accenture estimates that out of the projected 25 million patients impacted by health system data breaches, 6 million will suffer medical identity theft, and 16% of all data breach victims will have to cover out of pocket expenses related to that theft. The cost to patients is expected to be $56 billion over the next five years.

Unlike credit card theft, where credit card companies cover their customers' losses, there is no one to cover the cost of a medical identity theft. That makes it that much more important for health care systems to carefully protect their patients' data.

Lesson Learned:

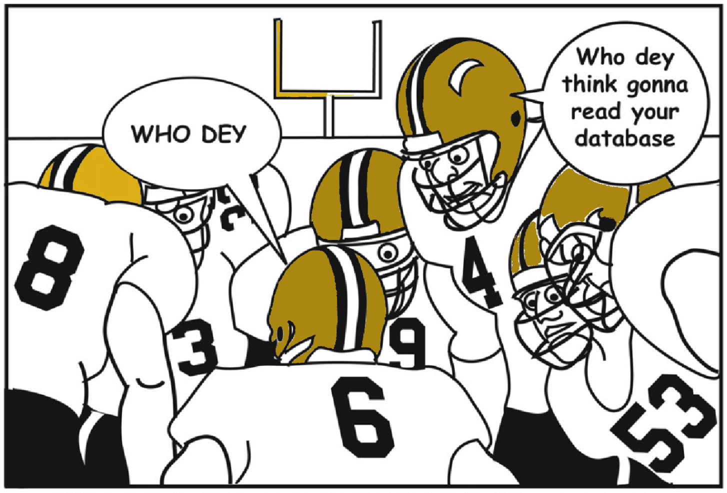
Be sure to familiarize yourself with and follow the HIPAA Privacy and Security policies. These policies were written to ensure protection of our patients' information, but are only effective if followed. If you have any questions about the policies, please contact Compliance or Information Technology for clarification.

Unsecure Email Causes Breach of 1,615 Patients

The North Carolina Department of Health and Human Services (NCDHHS) is alerting 1,165 patients after an employee sent an email containing a spreadsheet that contained patient information. While there was no indication that the email was intercepted or viewed by anyone other than who was intended to see the email, it is still considered a breach since email (unless encrypted) is not a secure method of transmission. NCDHSS has a policy to encrypt all PHI that is emailed, but the policy was not followed in this instance. Information exposed included Medicaid services provided to patients, provider names, Medicaid identification numbers, and patient names.

Lesson Learned:

LSU HCSD has a strict policy against sending **any** PHI over the email system, except a patient's medical record number **or** account number, and the patient's initials. In the event that PHI needs to be communicated inside or outside the LSU system, Liquid Files, a secure, encrypted email system may be used. Contact Information Technology should you need access to Liquid Files.



Cybercriminals want to know who is in your database. Maintain safeguards as a defense!

If you have any HIPAA questions or concerns, contact your Compliance Department at LAK (985) 878-1639 or ABO (225) 354-7032.