November 2015

Volume 1 Issue 11

Because We Care, We're HIPAA Aware

HIPAA Advisor

Question:
What is the difference between HIPAA Privacy and HIPAA Security?

Answer:
HIPAA Security and privacy are distinct, but go hand-in-hand.

The Privacy rule focuses on the right of an individual to control the use of his or her personal information. Protected health information (PHI) should not be divulged or used by others against their wishes. The Privacy rule covers the confidentiality of PHI in all formats including electronic, paper and oral.

Confidentiality is an assurance that the information will be safeguarded from unauthorized disclosure. The physical security of PHI in all formats is an element of the Privacy rule.

The Security rule focuses on administrative, technical and physical safeguards specifically as they relate to electronic PHI (ePHI). Protection of ePHI data from unauthorized access, whether external or internal, stored or in transit, is all part of the security rule. Typically ePHI is stored in:

- Computer hard drives
- Magnetic tapes, disks, memory cards
- Any kind of removable/ transportable digital memory media
- All transmission media used to exchange information such as the Internet, leased lines, dial-up, intranets, and private networks

Privacy Facts

Becky Reeves & Trish Rugeley
Compliance & HIPAA Privacy Officers

Use of PHI in Training

PELICAN is a complex system that requires significant training to be proficient in its use. It may also involve review of certain workflows when working with a group of co-workers to trouble shoot issues or demonstrate workflow changes. When that training or trouble shooting occurs, it is important to protect PHI as much as possible. The preference is to use test patients so that no actual patient's information is shared. When that is not possible, use the minimum necessary information possible to get the job done. HIPAA requires that when using or disclosing PHI we must take reasonable steps to limit uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose of the task. Complying with HIPAA is not always convenient, but it is necessary!

LSU HCSD Policy 4565

Information Technology Violations & Disciplinary Action

LSU HCSD has numerous policies that help protect both you, the user, and our patients. To locate these policies go to the LSU HCSD website – www.lsuhospitals.org - click on Employees, then select HCSD policies.

LSU HCSD Policy 4565- Information Technology Violations and Disciplinary Actions has been added to the HCSD policy website. This policy outlines possible disciplinary action should an employee be found to have violated LSU HCSD's HIPAA or Information Technology policies. The policy provides for violation levels and corresponding recommended disciplinary actions. **Please review the policy if you have not already done so.**

Security Facts

Public Wi-Fi Part 1

James "Mickey" Kees
Chief Information Officer / HIPAA Security Officer

It may be seldom that you ever need to use a Public Wi-Fi network when performing your work duties. When working remotely, you should be using the LSU VPN (Virtual Private Network) which allows you to communicate private information securely over a public network. But if for some reason you do not have access to a VPN, or you are doing some personal tasks, here are some helpful tips for using public Wi-Fi Networks.

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, and other public places are convenient, but are often not secure. If you connect to a Wi-Fi network, and send information through websites or mobile apps, that information might be accessed by someone else. To protect the information you are working with, only send information to sites that are fully encrypted, and avoid using mobile apps when working with PHI, personal, or financial information. To identify an encrypted website, look for **https** at the start of the web address. Some websites use encryption only on the sign-in page, but if any part of your session is not encrypted, your entire account could be vulnerable. Look for **https** on **every** page you visit if you need to protect information.

Unlike websites, mobile apps do not have a visible indicator like https. Many mobile apps do not encrypt information properly. If you must use an unsecured wireless network for communication/transactions via an app, use the company's mobile website- where you can check for the **https** at the start of the web address – rather than the company's mobile app.

Source: Federal Trade Commission

Connecticut Fines Hospital for HIPAA Violations, including Lack of Business Associate Agreement

In June 2012, EMC Corporation, a business associate of Hartford Hospital in Connecticut, reported that an unencrypted laptop was stolen from the home of an EMC employee who was doing data analysis for a quality improvement project. The laptop contained PHI of 8,883 individuals and was never recovered. The laptop included the individual's names, dates of birth, Social Security numbers, Medicaid and Medicare numbers, medical record numbers, and certain diagnosis and treatment information, all considered PHI under HIPAA. The settlement document between Hartford Hospital and the Connecticut State Attorney General noted that the hospital did not have a Business Associate Agreement with EMC Corporation, as required by HIPAA.

The State of Connecticut fined Hartford Hospital $90,000 for the HIPAA violation, and the hospital also entered into a "voluntary compliance assurance agreement" with the state. Part of that agreement included greater training for Hartford Hospital staff in recognizing when a BAA is required.

Lesson Learned:

LSU HCSD policy requires that all mobile devices be encrypted. In addition, it is vitally important that anytime LSU HCSD or Lallie Kemp Medical Center is working with an individual or company that will be receiving, accessing, storing or transmitting ANY PHI that we have a Business Associate Agreement.

Class Action Lawsuit in Washington D.C. Alleges HIPAA Violations in Allowing Patient Access to Medical Records

Two Washington D.C. hospitals have been named in a class action lawsuit related to patients being able to receive copies of their medical records. HIPAA states that healthcare providers may impose reasonable, cost-based fees for the copying and postage of requested medical records. However, in the lawsuit, it is alleged that the third party company contracted by the hospitals to do the release of information for this copying of medical records charged one patient $1,168 for his medical records, and another $1,558. The charges were for per-page copying fees, as well as a "basic fee" of $22.88 and a shipping and handling fee of $16.38.

Electronic health records have reduced the time and labor necessary to produce copies of medical records, but has significantly increased the number of pages that may be printed, which may have led to the extreme cost of the records.

Lesson Learned:

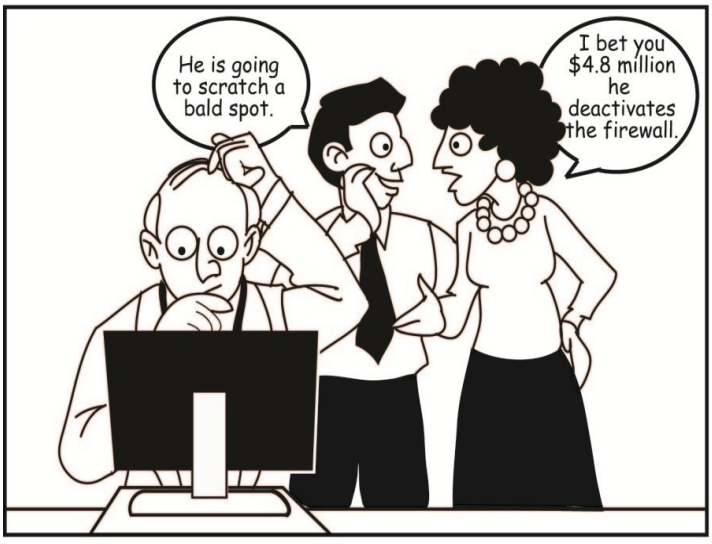
We must ensure that our costs to provide medical records to our patients are not artificially increased due to the amount of paper produced when printing an electronic health record. Louisiana facilities are governed by LA St.ate statue R.S. 40:1165.1 which limits the charge to no more than one dollar per page for the first twenty-five pages, fifty cents per page for twenty-six to three hundred fifty pages, and twenty-five cents per page thereafter.

Ex-Practitioner Exported Patient Information to New Employer

A former Baptist Health provider allegedly exported patient information to his new employer, a family practice clinic. In August, 2015, a Baptist Health patient complained that they had received unwanted solicitations from the family practice clinic, a clinic never visited by the patient. Additional patients came forward, noting that they were given the option to switch providers during the solicitation. An investigation into these complaints revealed that patient lists had been accessed and exported, without authorization or knowledge of the patients or Baptist Health, along with contact information for those patients.

Lesson Learned:

Users may only access patient information for Lallie Kemp or LSU HCSD treatment, payment, or healthcare operations. The access of patient information for personal gain is strictly prohibited by LSU HCSD policies, as well as HIPAA regulations.



"HIPAA monitoring can detect inadvertent re-configurations!"