HEALTH CARE SERVICES DIVISION

JANUARY/FEBRUARY 2016

HIPAA Advisor

Because We Care, We're HIPAA Aware

VOLUME 2, ISSUE 1

PRIVACY FACTS

Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

CHANGES TO THE HIPAA ADVISOR

The HIPAA Advisor has been providing HIPAA Privacy and HIPAA Security News and Education for over a year now! We appreciate you taking the time to review the information provided and putting it into action. Now that we have a solid foundation of HIPAA knowledge, the HIPAA Advisor will be moving to a bi-monthly publication. If there are subjects that you would like to see covered in the HIPAA Advisor please let us know! We want this newsletter to be informative and as effective as possible in helping us all be more HIPAA AWARE!

PAPER PHI IS MORE SUSCEPTIBLE TO BREACH THAN ANY OTHER MEDIUM

Even though much of the Protected Health Information (PHI) is stored electronically now, there is still plenty of paper that contains PHI found throughout our building. Sometimes we even forget that we have paper with PHI stashed in various places, so it is important to think carefully about where we keep our PHI, and take precautions when clearing out an area, as well as storing and transporting paper with PHI. Some things to consider include:

- When exchanging office furniture, make sure you clean out the entire piece so that you do not mistakenly leave paper with PHI in the drawers or cabinets. You should have a process that your staff follows whenever such furniture is leaving the department that ensures that no paper will be left behind. Desks and filing cabinets are at particularly high risk of having paper PHI left in them.
- When storing files of patient information, make sure that the storage area is secure and locked. It would not be secure to leave the files in an area accessible to those not authorized to have access to the records. For example, you would not store quality reviews that contain patient information in a public hallway alcove or in an unused and unlocked office.
- When transporting paper, enclose it in an envelope or covered container if practical. Be careful about setting paper down in a public area to perform another task, even momentarily. You would be surprised how many times paper PHI is found by or in a bathroom!
- Avoid bringing any paper with PHI home, and don't keep paper PHI in your car.

Paper PHI is the number one type of PHI that is breached at most health care institutions. Make sure it is protected!!

SECURITY FACTS

James "Mickey" Kees

Chief Information Officer / HIPAA Security Officer

BEWARE OF PHONE SCAMMERS

Hackers are calling businesses and homes, pretending to be from IT Support or from seemingly legitimate businesses such as Microsoft or Windows help desks. They will claim that something is wrong with your computer, and ask you to work with them to solve the problem. They may ask you to install software so that they can work on the issue. What they are really doing is installing malicious software that can corrupt your computer, and give them access to your user name and passwords! Sometimes the scammers will direct you to a website to download software, or even send you to a legitimate site to download remote desktop capabilities.

Remember that our IT Staff and Computer Vendors like Microsoft will NOT call you directly asking you to download software.

If you get a call from someone claiming to be contacting you because of a problem with your computer, tell them to contact our IT Department. Hang up with them as quickly as possible and immediately notify our IT Department of the call. Do not, under any circumstances, follow any instructions given to you by this person, no matter what dire circumstances they may describe will happen. Remember these instructions at home too, as home computers are being targeted by scammers as well. Be aware that scammers can be particularly persistent. You may get multiple calls. But follow these simple steps to keep our IT systems safe!

If you do happen to fall victim to a scammer, take the following steps:

1. Immediately turn off your computer and unplug it. If you are on wireless device, disable your wireless connection.
2. Contact IT immediately and report what happened. You may be given further instructions from there.

LSUHealth

Phone Scam Leads to Breach of Nearly 21,000 Individuals

Blue Shield of California sent out a breach notification letter informing some of its customers that their names, addresses, Social Security numbers, and dates of birth may have been exposed. Blue Shield became aware of the breach in December, 2015, when it learned that one of its vendors who provides enrollment assistance fell for a telephone scam, resulting in the scammer gaining access to log-in credentials of an employee of the Blue Shield data system.

Lesson Learned

Beware of phone scammers! See the article in the HIPAA Security Section!

Hospital That Was Victim of Phishing Attack in April 2015 Has Another Compromised Account

In April, 2015, Brigham and Woman's and Brigham and Women's Faulkner hospitals reported a HIPAA breach when a successful phishing incident compromised patient data. Those same two hospitals are now reporting another incident that has breached patient information. While the hospitals are not stating how the breach occurred, a statement on their website states that they learned that an unauthorized user obtained the network credentials of one of their employees, allowing the hacker to access the employee's email account. After investigation, it was determined that some of the emails of that employee contained patient PHI.

Lesson Learned

Despite the protections LSU HCSD has in place, there is always the risk that a hacker can gain access to our emails. That is one reason why LSU HCSD **prohibits** patient PHI in emails, other than an account number OR a medical record number and a patient's initials. Please pay particular attention to email strings and attachments that may contain patient information that you may unwittingly forward as you reply to emails. Remember that LSU HCSD has a SECURE email product that can be used if you need to send PHI. Contact your IT Department for more information.

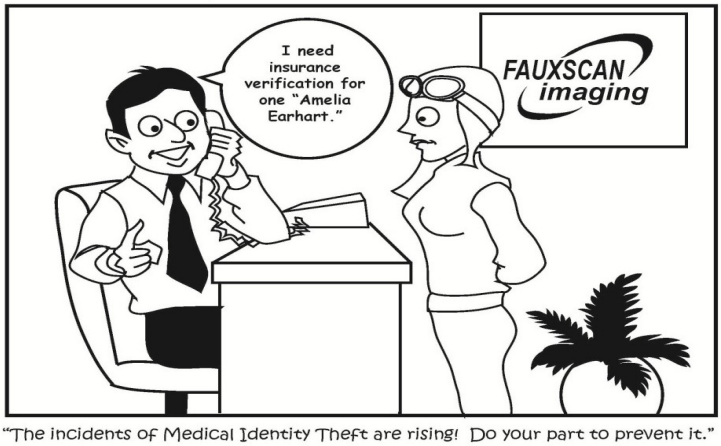
Theft and Loss of Unencrypted Mobile Devices Continues to Place Patients' Information at Risk

St. Luke's Cornwall Hospital in New York reported that an unencrypted USB drive was stolen from a restricted area within their hospital. The USB drive contained the PHI of 29,156 patients, including their names, medical record numbers, dates of service, and types of imaging services received. The Hospital noted that it will be working to ensure that all of its USB drives are encrypted, and that they will be moving towards technology that does not require the use of thumb drives or other mobile electronic storage devices.

Indiana University Health Arnett Hospital also experienced the loss of an unencrypted storage device. The device went missing from their Emergency Department and contained spreadsheets of patient information from 29,324 patients who had visited the ED over a one year period. The spread-sheets included patients' names, birthdates, ages, home phone numbers, medical record numbers, dates of service, diagnoses, and treating physicians. The theft or loss of unencrypted storage devices continues to be a major contributor to breaches that contain large volumes of patient information. It is LSU HCSD's policy that any mobile device that contains PHI be encrypted.

Lesson Learned

Make sure you follow LSU HCSD policy and ONLY use mobile devices that are ENCRYPTED when PHI is stored or accessed. Remember mobile devices include USBs, laptops, tablets, iPhones, disks, etc. Mobile devices are particularly prone to theft or loss. Always protect the physical security of mobile devices by keeping them in a secure location. As we can see from the stories here, just because the device is in a restricted area of the hospital does not necessarily mean that they are secure.



"The incidents of Medical Identity Theft are rising! Do your part to prevent it."

Paper Medical Records Stolen From Oncologist's Office

Illustrating how valuable patient information has become on the black market, thieves broke into the office of a California oncologist and stole paper medical records related to 1,300 patients. The information in the patient charts was enough to cause concern that patient identities were at risk. Thankfully, a number of the charts were recovered after the apprehension of a suspect, but not all. The charts stolen had patients' names, Social Security numbers, dates of birth, addresses, phone numbers, and the names of spouses, as well as height, weight, lab values, and blood pressure of patients. More detailed clinical information was kept in an electronic health record, and was not available to the thieves.

Lesson Learned

Patient information is valuable on the black market and is the target of thieves of all kinds. We must make sure that our paper with PHI is just as secure as our electronic medical records. While we may not think of patient information being a target, in this new age of identity theft, we must do all we can to protect our patients' paper PHI.

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