MARCH 2015

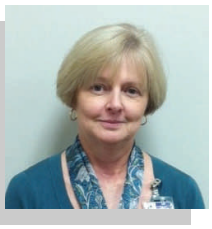
Because We Care, We're HIPAA Aware

HIPAA advisor

Volume 1 Issue 4

HEALTH CARE SERVICES DIVISION

PRIVACY FACTS



Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

RELEASE OF INFORMATION TO FAMILY OF PATIENTS

HIPAA allows the hospital to release general information to the family and significant others, but only when the patient does not object or has not had a history of objecting. The details of the HIPAA requirements are too numerous to list in this article, but here are a few tips.

1. HIPAA does allow us to discuss information with family members who are contacting us to assist with the payment of a patient's bill. However, you will want to keep any information you divulge to a bare minimum to achieve your objective. For example, if a family member calls to ask how much a patient still owes on the bill because the family member is going to pay the remainder of the balance, only discuss the balance amount, and not diagnoses related to the claim.
2. It is best practice to get the patient's permission to discuss anything more in depth with their family if it is information beyond a payment amount. You can ask to speak to the patient to receive verbal permission. Always document that permission.
3. Patients have the right to withhold information from their family, unless a family member has a legal designation to act as the patient's personal representative. A personal representative is someone legally designated by either being the legal guardian of an unemancipated minor, or designated as such through a legal power of attorney or healthcare power of attorney.

If you are ever unsure of how to handle a situation, PLEASE CALL COMPLIANCE and we will help you through!!!

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: If I am unconscious or not around, can my health care provider still share or discuss my health information with my family, friends, or others involved in my care or payment for my care?

Answer: Yes. If you are not around or cannot give permission, your health care provider may share or discuss your health information with family, friends, or others involved in your care or payment for your care if he or she believes, in his or her professional judgment, that it is in your best interest. When someone other than a friend or family member is asking about you, your health care provider must be reasonably sure that you asked the person to be involved in your care or payment for your care. Your health care provider may share your information face to face, over the phone, or in writing, but may only share the information that the family member, friend, or other person needs to know about your care or payment for your care.

Here are some examples:

- A surgeon who did emergency surgery on you may tell your spouse about your condition, either in person or by phone, while you are unconscious.
- A pharmacist may give your prescription to a friend you send to pick it up.
- A doctor may discuss your drugs with your caregiver who calls your doctor with a question about the right dosage.

BUT:

- A nurse may not tell your friend about a past medical problem that is unrelated to your current condition.

P2 How to Recoginize Phishing Attempts

P3 Lost or Stolens Mobile Devices

P3 Policy Spotlight— Use and Disclosure of PHI To persons involved in Patient's Care

P4 HIPAA In the News

Meet LSU HCSD's New HIPAA Security Officer — Mickey Kees

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

Well Mickey is certainly not new to LSU HCSD, but Susan Arceneaux was serving as the LSU HCSD Security Officer until her much deserved retirement in February. Mickey is now taking on that role. He is supported by a great staff of I.T. professionals that are always there to help us through any I.T. emergencies we might have!

PHISHING

Just like the activity it is named after, phishing is an attempt to set the hook for unsuspecting users, hoping that a few will take the bait. Scammers who go on phishing expeditions will send users an official looking email, right down to logos or web addresses, asking you to click on a link or reply to the email. The scammer will then ask you for sensitive information, such as your user name and password; or personal information such as your social security number or credit card number.

Remember: LSU will never ask you to send them your password in an email. And if you get an unsolicited email at home from what looks like an official website, call the company first before responding. In most cases, the U.S. government or companies will not send you an unsolicited email asking for personal information. It should be a red flag to you that someone is up to no good! ***Do not click on any links, and do not respond to the email!***

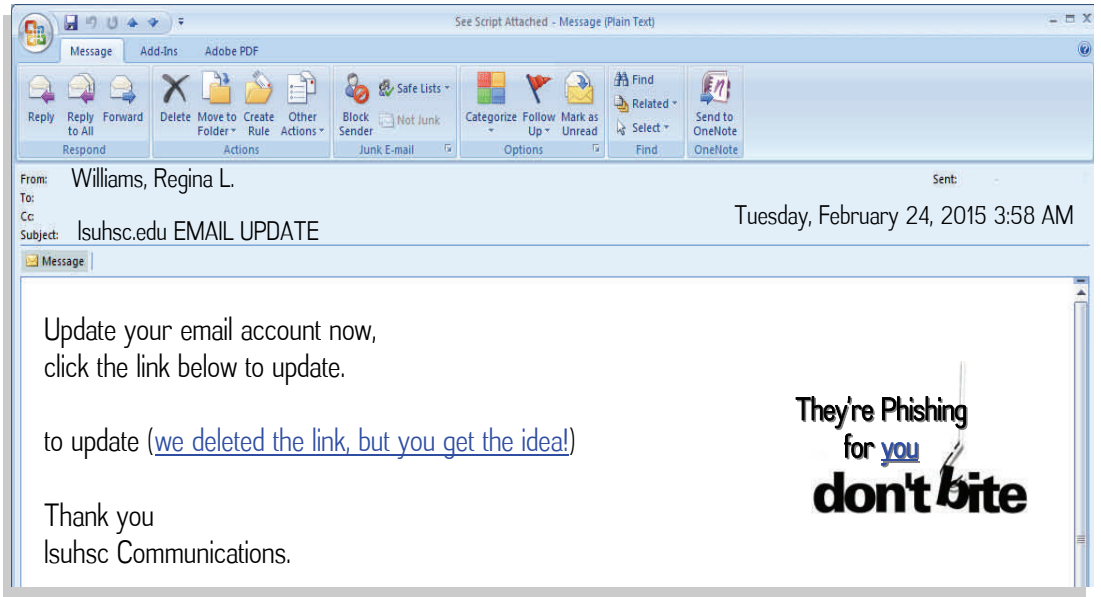
Should you get a suspicious email at work take the following steps:

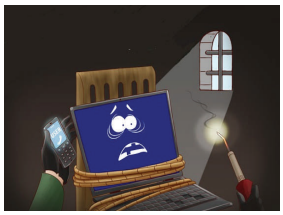
1. Send the email, **as an "attachment"** to Spam@lsuhsc.edu, and then **DELETE** the email from your Inbox.
2. If you do not know how to send as an attachment, contact I.T.

Just one person responding to such an email can put the whole LSU computer system at risk!

As a matter of fact, this example was an **ACTUAL PHISHING** incident that recently occurred!

An employee DID click on the link, and subsequently introduced a virus to our system.





RANSOMEWARE & CYBEREXTORTION

Ransomware is a type of malicious software that is designed to block access to a computer system until a sum of money is paid to release the data. It is a type of phishing scheme that depends on a user falling for the phishing attempt. If the user does click on a link, the hacker can send code that will lock the data and files on a server and encrypts that data so that the user can no longer access his or her own data. ***This is the type of phishing attack that LSU HCSD just experienced as shown in the example above.*** The bad news is, one of our employees clicked on a link from a phishing attempt, and the hacker introduced an encryption code. The good news is, the employee realized that something was wrong and warned I.T. so that I.T. was able to minimize the damage.

BEWARE: The largest HIPAA data breach to date, Anthem Healthcare, where 78.8 million individual's information was breached is thought to have started with a few employees falling for a PHISHING scheme.

SECURITY FACTS

LOST OR STOLEN MOBILE DEVICES

If you have a mobile device (e.g., laptop, smart phone, tablet) and you use it to access PHI in any format (e.g., reports, email, PELICAN, etc.) it is very important that you never save PHI directly to that device.

1. **IMMEDIATELY** report the missing device to your I.T. Security Officer! You may be tempted to wait to see if it shows up, but it is important to report it as soon as you know it is missing to protect the PHI as soon as possible.
2. If the device is stolen, report the theft to your local law enforcement agency.
3. If the device is a smart phone, contact your carrier (e.g., AT&T, Verizon, Sprint, etc.) and follow their instructions to secure the device.
4. Complete an incident report.
5. Notify your Compliance/Privacy Officer.

POLICY HIGHLIGHTS

LSU HCSD Policy 7514 – Use and Disclosure of Protected Health Information to Persons Involved in the Patient's Care and for Notification Purposes

LSU HCSD has numerous policies that help you protect our patient's PHI. To locate these policies go to LSU HCSD website – www.lsuhospitals.org - click on Employees, then select HCSD policies. The majority of the HIPAA policies are under section 7500.

Policy 7514 outlines, in general terms, when it is acceptable to share a patient's PHI with those involved in that patient's care, however; all LSU HCSD facilities and providers should provide the patient with an opportunity to agree to or object to the disclosure of their Protected Health Information to family members and other persons identified by the patient, or for notification purposes.

If the individual (patient) is present and has the capacity to make his or her own decisions, the Facility or Clinic may disclose the PHI to a family member, other relative, or a close personal friend of the patient, or for notification purposes only if the Facility or Clinic does one of the following:

(1) Obtains the individual's agreement in each encounter orally or in writing, to disclose the patient's Protected Health Information to the individual (e.g., family member, friend, other person) that is present with the patient; or

(2) Provides the individual with the opportunity to object to such disclosure, and the individual does not express an objection; or

(3) Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure

The policy also provides guidelines for release of PHI when the patient is not present or incapable of giving authorization, and guidelines for when the patient is deceased.

HIPAA TIME
Headlines That Matter to You

7,000 Veterans' PHI is Exposed By the VA

A vendor of the VA discovered a potential flaw in its data base, potentially compromising the PHI of Veterans who participated in home telehealth services. Due to the flaw, PHI such as names, addresses, dates of birth, and other similar data was potentially seen after the database was inadvertently exposed to the Internet. The security flaw in the vendor database was immediately corrected once discovered. The VA has been under scrutiny by the US Government Accountability Office (GAO) which pointed out concerns in the VA's cybersecurity policies and procedures.

Lesson Learned:

Healthcare providers must scrutinize their practices whenever there is the potential for a breach in data. Healthcare providers must also be careful to choose vendors who understand the importance of tight control over data, and have completed risk assessments that point out potential risks so that those risks can be mitigated.

Radiologist Arrested for Identity Theft

A New York radiologist is facing three misdemeanor charges after allegedly stealing information on 97,000 patients of the practice where he worked at the time of the incident. The radiologist told police that he accessed and copied the information because he was planning to start a competing medical practice. The radiologist allegedly connected an external hard drive to his workplace computer and copied the patient names, social security numbers, dates of birth, addresses and phone numbers, health insurance information, and diagnoses of patients in the data base of his employer. Also found on the hard drive was his employer's corporate credit card information, corporate marketing materials, and IT information. The radiologist may also be facing stiffer HIPAA penalties as the case is being reviewed. A loop hole in New York's state laws does not make the possession of this information an offense any greater than a misdemeanor. However, if prosecuted under HIPAA statutes, the physician faces much tougher consequences (a $250,000 fine and up to 10 years in prison).

Lesson Learned:

According to LSU HCSD policy, you can ***NEVER*** **download patient information to your own personal devices,** and certainly cannot do so for your own personal financial benefit.

Patient Discharged – Along with the Paperwork of Twenty Other Patients

According to television news in Denver, the Medical Center of Aurora in Colorado discharged a patient from an inpatient hospital stay. With her went the discharge paperwork of twenty other patients. The patient brought the other patients' paperwork back to the hospital, where a nurse took back the other patients' paperwork. But when the patient got home, she realized that she still had the operating room notes of seven other patients. The paperwork given to her included the patients' names, dates of birth, procedures, and medications.

Lesson Learned:

We know that the most common breach at Lallie Kemp is the unintentional handing over of paperwork with PHI to the wrong patient. Whenever you give a patient paperwork, that you:

- ***Verify that you have the right patient in front of you BEFORE you hand over any paperwork by using TWO IDENTIFIERS.***
- ***Go through each and every piece of paper to make sure each piece belongs to the patient you are about to give it to.***

Such a practice is a good idea for HCSD as well. If your job entails mailing PHI, make sure you have the right papers going to the right place. You can see how important it is that we follow this practice each and every time we hand over or mail papers containing PHI. The Hospital in Aurora is now having to cover the cost of identity theft protection for the persons whose PHI was compromised, and has tarnished their reputation.

Hospital Worker Sentenced to Two Year Prison Term

An Alabama hospital worker plead guilty to one count of aggravated identity theft, resulting in a two year prison sentence. The lab technician from Flowers Hospital in Dothan, Alabama stole patient records of 73 patients, using their PHI to file fraudulent tax returns and obtaining refunds from the IRS. The worker attempted to steal $536,000 worth of tax refund claims, but the IRS only actually paid out $19,000 before the scheme was discovered.

Lesson Learned:

Patient PHI is valuable to criminals and we must protect it from theft. If you ever suspect the unlawful use of patient PHI, report it immediately to the Compliance Office!