Because We Care, We're HIPAA Aware

HIPAA ADVISOR

Volume 1 Issue 6

MAY 2015

HEALTH CARE SERVICES DIVISION

PRIVACY FACTS

Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

Social Media

Our patients' information should NEVER be shared on any social media website.

Even if you do not mention the patient by name, those who know the patient may be able to piece together bits of information and determine the patient's identity. The sharing of patient pictures, descriptions of patients' illnesses and/or injuries, or stories about patients is strictly prohibited.

Safeguarding Paper with PHI

We seem to have more paper now than ever before, despite the electronic medical record environment. Paper with PHI has actually proven to be Lallie Kemp's primary HIPAA breach risk. We want to make sure it does not become such a high risk at LSU HCSD. So how can you keep that PHI safe?

- When mailing documents to a patient or patient's representative, make sure the name of the addressee matches the name on the paperwork you are placing in the envelope. Goal: RIGHT PATIENT received RIGHT PAPERWORK. We do that by checking EVERY piece of paper, and using TWO IDENTIFIERS to ensure that we are mailing the right papers to the right person.

- **Caution:** paperwork for multiple patients can become mixed up in a busy work space. That is why we have to go through EACH piece of paper to insure RIGHT PAPERWORK to the RIGHT PATIENT.

- If paper is to be discarded, make sure it does not have ANY PHI on it. If it does, it must go in the SHRED BIN.

- Some employees keep a container of paper to be shredded at their work station. Make sure these papers destined for the shred bin cannot be mistaken by housekeeping as trash. Clearly mark any such container as SHRED material.

SECURITY FACTS

Malware

James "Mickey" Kees

Chief Information Officer / HIPAA Security Officer

Malware is an all-encompassing term used to describe computer programs that are designed to damage you, your business, and/or your computer. It includes programs such as phishing, worms, Trojan horses, viruses, and spyware. LSU has multiple layers of malware protection, but that protection cannot guard against the most dangerous threat of all – human error.

Some things that you can do to protect LSU and yourself from malware:

- Make sure that you do not click on any suspicious links, attachments, or emails.
- Be on the lookout for phishing attempts. Such attempts try to lure you into responding to an email or clicking on a link, which will in turn introduce malware into our system.

If you use a LSU laptop or tablet, make sure it is connected to the LSU network at least once a week so that your device can receive malware protection updates.

Secure Workstations

HIPAA requires healthcare providers to physically secure their computer resources. One of the most common of these resources is your desktop computer. The two most important things that you can do to physically secure your computer are:

1. Make sure that you store any work on your "O Drive", instead of the hard drive of the computer. Documents stored directly on the hard drive of your desk top are vulnerable to loss or theft. If your work is stored on your O Drive, it is stored on a secure server and automatically backed up. If you are unsure if you are storing your information on your O Drive, contact your I.T. Help Desk for assistance. or contact IT.

2. Make sure that you LOG OFF or LOCK the screen when you leave your desk top computer. While sometimes inconvenient, logging off or locking your computer ensures that no one can come behind you and inappropriately access information. Remember, anything done under your User ID IS YOUR responsibility.

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: Why is the HIPAA Security Rule needed and what is the purpose of the security standards?

Answer: In enacting HIPAA, Congress mandated the establishment of Federal standards for the security of electronic protected health information (e-PHI). The purpose of the Security Rule is to ensure that every covered entity has implemented safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Standards for security are needed because there is a growth in the exchange of protected health information between covered entities as well as non-covered entities. The standards mandated in the Security Rule protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. The Security Rule establishes a Federal floor of standards to ensure the availability, confidentiality and integrity of e-PHI. State laws which provide more stringent standards will continue to apply over and above the new Federal security standard.

Health care providers, health plans and their business associates have a strong tradition of safeguarding private health information. However, in today's world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the Rule provides clear standards for the protection of e-PHI.

Lab Worker Fired After Divulging Lab Test Result of Pregnant Patient

The University of Iowa fired a lab technician at its student health center after the lab tech divulged the results of a pregnancy test that she had just processed. The lab tech also pointed out the boyfriend of the patient while he sat in the waiting room to the clerk working at that time. The boyfriend was a well-known student athlete. After the clerk learned of the pregnancy, she went to two additional co-workers and asked them details about the female patient.

The lab technician, who had been at the student health center for 14 years, was fired and the clerk was disciplined.

This is not the first time the University of Iowa has fired employees for inappropriate access. In 2011, three employees of the student health center were fired after they inappropriately accessed the medical records of 13 football players who had been injured in an off season workout.

Lesson Learned:
You may only access the protected health information (PHI) of patients that you have a direct treatment, payment, or operational need to know. Access for curiosity or gossip purposes is considered an inappropriate access, and will result in disciplinary action.

Don't let curiosity or gossip lead you down the wrong path!

Malware Causes Breach of Data Base Containing PHI

A dental provider notified 151,626 patients in Oregon of a breach involving the hacking of an internal database. The hacker accessed the database through a work computer infected with malware. The compliance manager of the dental provider speculated that the malware could have been introduced via an advertising banner as employees browsed the internet. However, the employee on the computer at the time of the infection had not been on email or any websites that would have been prohibited.

Lesson Learned:
Browsing the internet always has its risks. Make sure you are only accessing those sites that are work related. At least if malware is introduced from such activity, you would have been acting within LSU HCSD policy. In addition, if you have a laptop or tablet, make sure that you log in to the LSU HCSD network to ensure that your computer is updated.

Employees at Blue Cross in Michigan Arrested for Identity Theft

Eleven people have been charged with identity theft and credit card fraud after a Michigan Blue Cross employee allegedly printed and shared screen shots of more than 5,500 people insured with the company. Three of the accused allegedly purchased more than $742,000 worth of merchandise at Sam's Club using fraudulent credit cards opened with the stolen identity information.

Lesson Learned:
Be on the lookout for any suspicious activity of employees who have access to PHI.

Another Breach Caused by the Theft of Unencrypted Laptop

Information on more than 38,000 individuals was exposed when an unencrypted laptop and two unencrypted hard drives were stolen from a car parked in an Indianapolis parking lot for 2 ½ hours. The laptop and hard drives belonged to the Indiana State Medical Association, and contained information such as names, dates of birth, health plan numbers, and in some cases, Social Security numbers, along with medical information. While laptops are a common target, remember that ANY mobile device is at risk. Therefore, it is the policy of HCSD to *prohibit* storage of documents containing PHI on portable devices such as laptops, tablets, and smart phones.

Lesson Learned:
It is vital that all HCSD employees understand that PHI is not to be stored on any portable device (or desktops either), and that any portable device must also be encrypted. If you have any questions about this policy, please contact I.T.