HIPAA Advisor

Because We Care, We're HIPAA Aware

HEALTH CARE SERVICES DIVISION

VOLUME 1 ISSUE 8 | AUGUST 2015

PRIVACY FACTS

BUSINESS ASSOCIATES

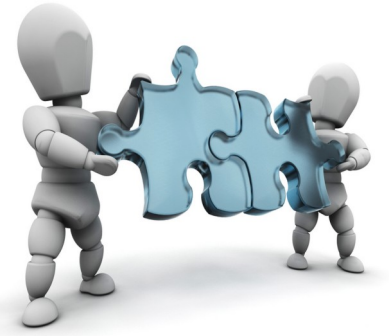
Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

A Business Associate (BA) is a person or company (other than a member of the hospital's workforce or treatment providers) that performs a service or activity on behalf of the HCSD or Lallie Kemp Medical Center **AND** has access to our patients' information. If the person/ company creates, receives, maintains or transmits patient protected health information on our behalf, then the person/ company is considered to be a BA. There has to be a fully executed Business Associate Agreement (BAA) **BEFORE** that person/company can have access to patients' information.

A significant purpose of the BAA is to define how the BA is to receive and use the PHI and to hold them accountable for compliance with HIPAA. Sometimes it is hard to determine who is and who is not a BA.

Whenever you are exploring a new purchase order, contract or arrangement that requires a person/company to have access to PHI, please contact the Compliance Department so that we can help you determine if a BAA is needed. Compliance will even write the BAA for you, and make sure the BAA is included in our up-to-date listing of all BAAs. Such a listing is necessary, because the Office for Civil Rights can ask for the list at ANY time.



Even if the person/ company does not meet the definition of a BA, there may still be a need to have some sort of document to protect patient information. Therefore, it is important that you notify compliance so that we can help you sort through this issue.

It is a violation of HIPAA regulations to not have a BAA when one is required, and LSUHCSD can be fined for noncompliance. So please help us stay in compliance with this regulation!

inside

LSUHealth

Increase in Junk Emails

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

Due to a change in our junk e-mail filter, HCSD has seen a significant increase in junk e-mails. Junk e-mails are also sometimes referred to as SPAM. Please treat these emails with extreme caution. They may contain viruses, phishing attempts, and other forms of malware. You can either delete the e-mail, or forward the e-mail as an attachment to Spam Reporting at spam@lsuhsc.edu. If you do not know how to forward an email as an attachment, please contact the Information Technology Department, and we will walk you through it. LSU Health Sciences Center Information Security Department (IS) manages our spam filter, and they are looking into remedies for the increased junk e-mail. In the meantime, IS will attempt to route all spam to your junk e-mail folder. If you are missing an expected e-mail, check you junk e-mail folder. Take care in reviewing items contained in your junk e-mail folder. We are depending on the HCSD users to use their HIPAA Security training to be smart about e-mails!

Downloading Software

This is a reminder that users should not be downloading any software to their computers. All software installed on computers at HCSD must be approved and installed by the Information Technology Department.

Please refer to the Management of Information Policy # 0141 for more information.

Security Facts

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: **When is a health care provider a business associate of another health care provider?**

Answer: The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a Covered Entity to a health care provider for treatment purposes.

Therefore, any covered health care provider (or other covered entity) may share protected health information with a health care provider for treatment purposes without a business associate contract. However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. For example, a hospital may enlist the services of another health care provider to assist in the hospital's training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to patient health information.

Policy Highlight

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.

LSU HCSD Policy 7510 Business Associate Agreements

LSU HCSD Policy 7510 outlines the procedure for identifying a Business Associate, including a decision matrix that employees can use to determine if a person/company would be considered a BA under HIPAA. It also includes a list of entities that are considered exceptions to the BA requirement. Finally, this policy provides the BAA template so that employees can see the requirements of a BA contract.

You can review the policy by going to http://www.lsuhospitals.org/new_hipaa_policies.aspx

UCLA Medical Center Hacked – 4.5 Million Records Potentially Exposed

UCLA Medical Center announced that cyber criminals were able to hack into their network that contained the records of up to 4.5 million people. UCLA is working with the FBI to investigate who is responsible for the hack, and what information may have been accessed. The cyber attack may have begun as early as September, 2014, and was discovered in October, 2014. However, it was not until May 5, 2015 that UCLA realized that the portion of the network that contained personal information such as names, Social Security numbers, medical record numbers, dates of birth, addresses and other sensitive information may have been accessed.

Such attacks are becoming more common, following the cyber attacks on Premera and Anthem Blue Cross which left the personally sensitive information of up to 89.8 million people vulnerable.

Lesson Learned:

Employees must always be on the alert for a potential scam designed to trick you into providing a way to hack into our computer information system. Beware of phishing attacks. Never respond to an e-mail from someone you do not know. Do not click on any links or pictures from those you do not know. Do not give out any information such as your password in a response to an e-mail, even if it looks official. Do not surf the web from work for non-work related purposes. If you have any doubt about an e-mail you receive, or the security of your computer, contact your Information Technology Department. And if you believe you have mistakenly provided access to a potential hacker, immediately notify your Information Technology Department so that they may investigate.

St. Elizabeth's Medical Center Receives $218,000 Fine for HIPAA Violations

St. Elizabeth's Medical Center in Boston has been fined $218,000 for two separate HIPAA security incidents that impacted a total of 1093 patients. In November, 2012, the Office for Civil Rights (OCR) received a complaint by the hospital's workforce members that some patients' PHI was being stored on an internet-based document sharing application without the proper security precautions to protect the information. St. Elizabeth's, though aware of the incident, did not report it in a timely manner to the OCR. Then in a separate incident on August 25, 2014, St. Elizabeth's reported that an unencrypted laptop and USB flash drive was lost. The combination of these two incidents, and the perceived slow response by St. Elizabeth's, lead to the large fine.

Lesson Learned:

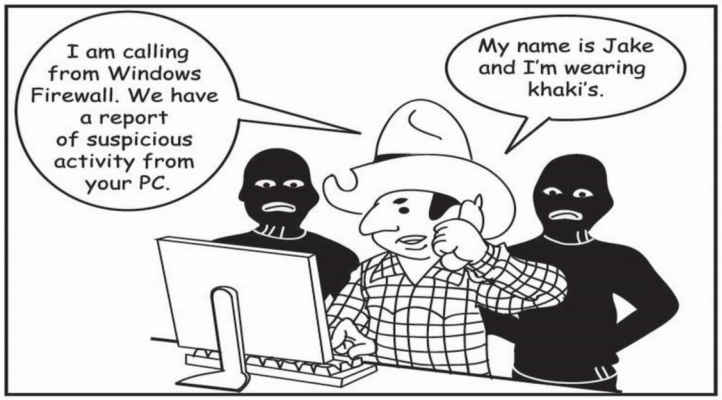
Potential HIPAA breaches must be reported promptly to the HIPAA Privacy Officer and/or HIPAA Security Officer so that the proper steps can be taken to notify OCR if a HIPAA breach is confirmed. PHI is not to be stored on laptops and all laptops should be encrypted. USB drives that store PHI must be encrypted. Finally, no patient information should be stored in an internet-based document sharing file unless the file is deemed by HIPAA Security to be secure after a comprehensive risk assessment, and permission is given by Information Technology to use the file.

Tweeting of NFL Pro's Medical Information Causes HIPAA Breach

Forbes is reporting that a hospital worker told a friend about New York Giants' defensive end Jason Pierre-Paul's injury after the NFL player was treated for injuries sustained in a 4th of July fireworks accident. The injury information was subsequently tweeted by ESPN reporter Adam Schefter, and eventually led to the withdrawal by the Giants of Pierre-Paul's $60 million contract offer. Included in the tweet was a picture of the player's medical record from Jackson Memorial in Miami, Florida. It is important to note that allegations that someone from the hospital leaked the medical record have not yet been confirmed by the investigation now underway. However, if the investigation reveals that the source of the breach was from Jackson Memorial, the hospital faces significant repercussions.

Lesson Learned:

Health care workers must remember that **no** information about a patient may be shared with those who do not have a treatment, payment, or operational need to know. If indeed a hospital worker told a friend about this player's injury, the worker most likely did not envision the string of events that would ultimately unfold. Even if you believe sharing a little bit of information about a patient is an innocent exchange between you and a friend, you cannot be sure where the information will go from there. The sharing of the information with a friend is a breach, and the liability of any further sharing will be on the hospital worker and the hospital itself.



"Be Wary of Phishing. Verify Credential before giving information."

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