JANUARY 2015

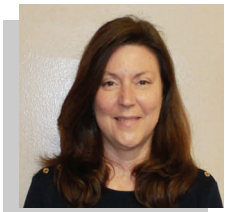
HEALTH CARE SERVICES DIVISION

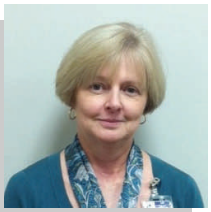
HIPAA Advisor

Because We Care, We're HIPAA Aware

PRIVACY FACTS

Volume 1, Issue 2





Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

Right of Access

HIPAA not only works to protect patient information, it also provides for specific rights of patients related to their own PHI. One of those rights is the right to access their PHI. Except in certain circumstances, individuals have the right to review and obtain a copy of their PHI.

While the rules about a patient's access are not complicated, there are several exceptions and procedures that must be followed.

Because of this, all patients' requests to access or copy their medical records should be forwarded to the Health Information Management (HIM) for processing. The important thing for our employees and medical staff to remember is that if a patient requests access to his or her medical record, then the patient should be directed to or assisted to contact Health Information Management (HIM). One of the reasons why the Office for Civil Rights investigates providers is because providers refuse the patient access to his or her medical record.

Privacy Complaints

HIPAA requires health care providers to address the complaints and concerns of patients and others about the security and privacy of PHI. LSU HCSD has two individuals that can process HIPAA complaints and concerns. Trish Rugeley and Becky Reeves, our Privacy Officers, can process any patient concerns or complaints regarding HIPAA.

What is PHI / PII / ePHI?

The crux of HIPAA security and privacy is the protection of PHI. But what is PHI anyway?

- **Protected Health Information (PHI)** is any individually identifiable health information (PHI) held or transmitted by a provider or its business associates, in any form or media, whether electronic, paper, or oral. This information, including demographic data, is related to the patient's health status, the provision of health care to the patient, and the payment of the care provided to the patient.
- **Personally Identifiable Information (PII)** is information that can be used on its own or with other information to identify a single person or to identify an individual in context. PII is a subset of PHI, and includes 18 individual identifiers that are specifically protected by HIPAA. Those 18 identifiers include
    - Patient name, social security number, address, any geographical subdivision smaller than a state, phone number, email or other social media identifiers;
    - Date of birth, date of service, date of discharge, date of death, and all ages over 89;
    - Hospital account numbers, medical record numbers, health plan identification numbers, credit card numbers, checking account numbers;
    - Full face photographs or other identifiable photographs (think tattoos, scars, etc.), finger-prints, or other bioidentifier;
    - Driver license number, vehicle registration numbers, license plate numbers;
    - Any other unique identifying number, characteristic, or code
- **Electronic Protected Health Information (ePHI)** – is PHI that is held in electronic form, such as in your computer or on PELICAN.

Also Inside this issue:

LSUHealth

Susan Arceneaux
IT Director /
HIPAA Security Officer

The HIPAA Security Rule requires healthcare providers to do a detailed analysis of where the risks to our electronic PHI might be, as well as develop plans to lessen or remove those risks. This means that EVERY system that may hold PHI electronically must be assessed, right down to individual employee and medical staff member data bases. If you happen to have such a database, please let your HIPAA Security Officer know so that we can include it in the HIPAA Risk Analysis!

Tips to Protect ePHI

Speaking of the risks to ePHI, the most common LARGE breaches involve electronic PHI (ePHI). Take the following steps to make sure that the ePHI you are using is protected:

- Never share your password with anyone! Do not write your password down and place it around your workstation for others to use or discover.
- Do not store patient information on mobile devices.
- Do not leave computer screens containing patient information open when you are away from the computer. Log Off!!
- All electronic devices should be secured at all times. Lost or stolen electronic mobile devices account for the majority of reported breaches in the United States, and are a prime target for thieves.
- Do not store PHI in unsecured files, and do not store PHI on the hard drive of your computer.
- If you get a suspicious email, call Information Technology right away for assistance.
- Remember you will never receive an email from LSU asking for personal information, your password, etc. If you get such a communication, notify Information Technology immediately.
- Do NOT send PHI through the LSU or any other email system. **Remember—**for business purposes within the LSU information system (example, among fellow CBO employees)-we can use a patient account number OR medical record number and initial but no other PHI may be sent via and email.
- Never send PHI through a text!

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.

Q: If someone has health care power of attorney for an individual, can they obtain access to that individual's medical record?

A: Yes, an individual that has been given a health care power of attorney will have the right to access the medical records of the individual related to such representation to the extent permitted by the HIPAA Privacy Rule. HOWEVER, when a physician or other provider believes that an individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse or neglect by the personal representative that holds the health care power of attorney, or present any danger to the patient as a result, the physician/provider may choose to not allow the personal representative access to the medical record.

Policy Spotlight
Shedding Light on Policy

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

LSU HCSD Policy 7503 - Patient's Right of Access to and Obtain a Copy of Their PHI

This policy outlines the right of a patient to access his medical record, and obtain a copy of that medical record. Some of the highlights of this policy include:

- If a patient would like to access his medical record, the patient should be assisted to contact the Medical Record department of the treating hospital for such access. The Medical Record department can help the patient get a copy of his medical record as well.
- HIPAA requires the treating hospital to give the patient access to his medical records, with very few exceptions. If the hospital denies the patient access to his record, then the patient must be informed of this in writing, outlining why the access was denied, and giving the patient the right to appeal that denial, if certain criteria are met.
- The hospital must respond to the patient's request for access within 15 days.
- The patient has the right to get a copy of his medical records in paper or electronic format, which ever the patient prefers.
- The patient may also direct the hospital to send his medical records directly to a third party if this request is made in writing by the patient.

HIPAA in the News: *Headlines That Matter to You*

TOP Breaches of 2014

The Department of Health and Human Services maintains a ***"Wall of Shame"*** that lists major breaches that involved 500 or more patients in any given breach. As of December 23, 2014, there were 1,186 major breaches impacting a total of nearly 41.3 million people since the HIPAA Breach Notification Rule went into effect in 2009. The top five breaches in 2014 affected nearly 7.4 million people. The following were considered the largest breaches of 2014.

#1 – The hacking attack on Community Health System, which affected 4.5 million people. It is believed that hackers originating from China used sophisticated malware to attack this hospital chain's systems.

#2 – The legal dispute between Texas Health and Human Services Commission and Xerox. The breach occurred when Texas Health ended its contract with Xerox, but Xerox failed to return computer equipment and paper records that contained the PHI of 2 million individuals. With no Business Associate Agreement or contract, Xerox allegedly maintained possession of PHI without a need to have the information, leading to the opinion that a breach occurred.

#3 – The theft of eight unencrypted **desktop** (yes, desktop – not laptop) computers from an office of a patient billing and collection service, Sutherland Healthcare Services. The desktop computers contained information of more than 342,000 people.

#4 – The unsecure computer folder that was inadvertently left accessible via the Internet. Touchstone Medical Imaging, a provider of diagnostic imaging services became aware that a seldom-used folder containing patient billing information of more than 307,000 patients could be viewed over the Internet.

#5 - The unauthorized access of patient information at the Indian Health Services, a federal agency. This breach affected 214,000 when an employee left a computer folder with PHI open and accessible in the public computer domain.

These breaches provide valuable lessons to health care providers and their employees on how to protect patient PHI. LSU HCSD and Lallie Kemp depend highly on its employees to be well educated and compliant with PHI protection, since employees' actions are often responsible for major breaches. So, remember those tips to protect PHI so that Lallie Kemp does not end up on the Wall of Shame!

Why You Must Protect Those Mobile Electronic Devices

The Massachusetts attorney general just fined Boston's Children's Hospital $40,000 for a breach that involved a stolen laptop in 2012. The incident occurred when a physician of the Children's Hospital brought his unencrypted laptop to a conference in Buenos Aires. Before the laptop was stolen, a colleague sent the physician an email that contained the PHI of 2,149 patients.

The physician believed that he had taken steps to remove the PHI from his email. However, the PHI actually remained on the laptop, and because the laptop was not encrypted, the PHI was compromised.

Lesson Learned: PHI should NEVER be sent via the email and PHI should not be stored on any computing device. Most importantly, any portable computing device must be encrypted if it is going to be used to work with PHI.

If you have any HIPAA questions or concerns, contact your Compliance Department at (985) 878-1639