HIPAA advisor

Because We Care, We're HIPAA Aware

VOLUME 1 ISSUE 7 JUNE / JULY 2015

HEALTH CARE SERVICES DIVISION

PATIENT'S RIGHT TO RESTRICT COMMUNICATIONS

HIPAA provides patients the right to restrict who Lallie Kemp/HCSD communicates with in regards to treatment, payment, or healthcare operations. To request such a restriction, patients must complete the form found in LSU HCSD HIPAA Policy 7504.

The written request must be sent to the HIM Director or HIM Custodian for review. If the HIM Director or HIM Custodian does agree to the restriction, then everyone at Lallie Kemp and LSU HCSD have to abide by the restriction. If the HIM Director or HIM Custodian does not agree to the restriction, then the patient has to be notified in writing.

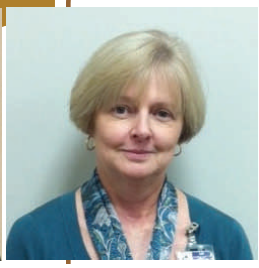
Examples of restrictions for communication include, but are not limited to:

- Not sharing the patient's information with a particular Lallie Kemp employee because the patient believes that employee will use the information to harm them;
- Asking that we not share the patient's diagnosis with a particular family member, even though that family member is usually very involved in the patient's care.

This right as outlined by HIPAA can be very confusing. It allows patients to request restrictions for the specific purposes of treatment, payment, or healthcare operations, but does not require the hospital to comply with the request. In the very same rule, however, HIPAA requires hospitals to allow patients to demand that the hospital not communicate with their insurance payer if the patient agrees to pay for a service out of pocket, and the hospital must honor that demand if certain criteria are met. And we know that we would not share a patient's information with the patient's family or friends unless the patient gave the hospital permission to do so, even if the form is not completed. Thankfully, it is rare that a patient evokes the right to restrict communications. But it is important to understand what we must do if such a situation occurs.

PRIVACY FACTS

PATIENT'S RIGHT TO ALTERNATIVE COMMUNICATIONS



Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

HIPAA provides patients the right to request that Lallie Kemp and LSU HCSD communicate with them in a confidential manner by specifying an alternate location or method for that communication. If the hospital or LSU HCSD can accommodate the request, then we are required to honor that request. Examples of such requests include, but are not limited to:

Alternate Location—Request that LAK/HCSD contact the patient by

- Using their cell phone number instead of their home number
- Sending test results to a P.O. Box or alternate address instead of the street address.

Alternate Method—Request that LAK/HCSD contact the patient by

- Only sending information in a plain envelope.

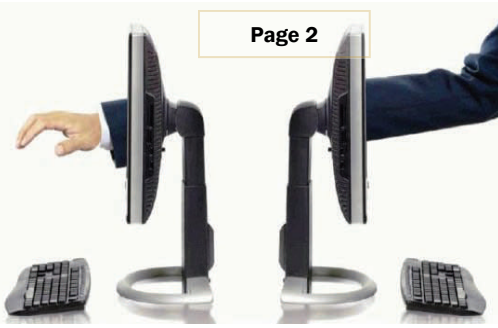
If a patient requests such confidential communications, the patient must complete the form found in LSU HCSD Policy 7506. The completed form should become part of the patient's medical record. Such requests are rare, but do happen. Staff should be on the lookout for any such requests when calling or mailing information to patients.

inside

LSUHealth

REMOTE ACCESS

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



PHI can be particularly vulnerable when it is being accessed away from the office. Remember to only use secure pathways when accessing PHI by going through either Citrix or VPN. Keep the PHI that you are working with remotely to a minimum if possible. NEVER save any PHI to your personal devices such as a home computer or tablet. Do not print PHI from home or hotel printers. And be aware of your surroundings when you are working with PHI away from the office; do not let any unauthorized viewer see PHI when working in a public environment.

Questions about these guidelines? Contact your I.T. department for further information.

PROHIBITION OF OUTSIDE DATA STORAGE

Recent breaches in the news have highlighted the importance of being aware of PHI that might make its way to personal computing devices. To avoid such incidents, never store PHI on any computer device, especially not any personal computer device such as a home computer, laptop, tablet, smart phone, flash drive or external hard drive. It is against LSU HCSD policy to send PHI in emails, but it is especially important not to send emails containing PHI to your personal email account. Personal computer devices will likely not have the same level of security that LSU computing devices do, and the sanitization and disposal of such devices at the end of their life will not be as robust.

HIPAA TIME

Headlines That Matter to You

EMPLOYEES WHO EMAIL PHI TO A PERSONAL ACCOUNT CAUSE HIPAA BREACH

The **Metropolitan Hospital Center (MHC)** in New York has issued breach notification letters to 3,957 patients after it was discovered that an employee emailed their PHI to a personal email account. This is the third such breach for the corporation that owns MHC this year. The **Jacobi Medical Center** sent a breach notification to 90,060 patients when an employee emailed PHI to a personal email account. And **Belleview Hospital Center** sent breach notification to 3,334 patients when an employee emailed a spreadsheet containing PHI to a relative. While the report of these breaches does not specify that the emailing of the PHI was for personal use or illegal activity, there is the question of the security of the data since it was sent outside of the hospitals' information security network.

Lesson Learned: LSU HCSD and Lallie Kemp have a policy against emailing patient PHI so that such information can be protected. According to the policy, only an account number ***OR*** medical record number, and the patient's initials may be emailed. It is best to not include detailed, sensitive clinical data in that same email. It is never permissible to send patient information to a personal email account. Any PHI sent to other individuals must be for a BUSINESS reason, and must be sent securely. If you ever need to send such a file, contact I.T. for assistance.

IDENTITY THEFT RING STEALS IDENTITY OF 13,000 PATIENTS

An employee of Montefiore Medical Center in New York was instrumental in gathering patient information that was then used to open up fraudulent store credit cards to make purchases. The employee was a clerk at the hospital, and had access to PHI of patients that she then passed on to the identity theft ring leader. The stolen information was then allegedly used to open credit card accounts at stores like Macy's, Zales, and Lord & Taylor. The employee's involvement was discovered as authorities were investigating the identity theft ring. The employee has been charged with one count of felony grand larceny and one count of felony unlawful possession of personal identification information.

Lesson Learned: Please report any suspicious activity of a co-worker related to PHI access or printing. LSU employees who were aware of their surroundings have been instrumental in assisting LSU in discovering unauthorized access of PHI over the years.

EMPLOYEE LOSES LIST OF PATIENTS -LIST FOUND IN NEIGHBORHOOD DRIVEWAY

An employee of Orlando Health accidentally brought home a list that included the patient names, diagnoses, and medical record and account numbers of sixty-eight patients. The list was later found in a neighborhood driveway after being lost by the employee. While the investigation revealed that it was purely an accident, Orlando Health was still required to send out breach notification to those sixty-eight patients. This is the second reportable breach by Orlando Health in a year's time. Last year, Orlando Health reported the loss of a flash drive containing the PHI of 586 children.

Lesson Learned: PHI in all of its forms must be protected! Ensure that you do not bring any PHI home. If there is a legitimate business need to bring PHI home, make sure your supervisor is aware, and that all precautionary steps are taken to protect the information until it can be safely stored in the work environment. Lallie Kemp is also moving toward a procedure in which only HOSPITAL ISSUED flash drives will be allowed. These flash drives will be encrypted, thus ensuring the security of the data contained within them.