Because We Care, We're HIPAA Aware

HIPAA Advisor

HEALTH CARE SERVICES DIVISION

VOLUME 1 ISSUE 12

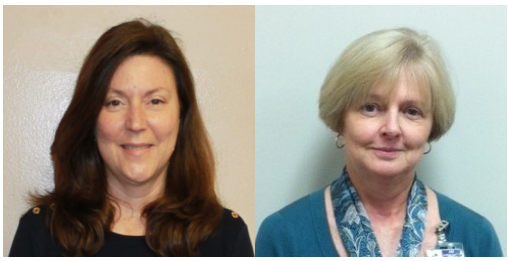
DECEMBER 2015

SECURE FAXES

The beginning of a new year is always a great time to do a little housekeeping for the year ahead. Now might be a great time to check your fax machines to make sure that your department is taking all of the necessary precautions to protect faxes that contain PHI. Some of those housekeeping items include:

1. Make sure that you have an updated Cover Sheet that contains a Confidentiality Statement and instructions to contact you if the fax is sent to the wrong person. Cover sheets must be used on all faxes, even those sent in-house.
2. Validate any pre-programmed fax numbers. Fax numbers can change over time. It is important that you periodically validate those numbers, particularly if they are numbers that you do not use often.
3. Fax machines that receive PHI should be in a secure location so that unauthorized persons do not have access to any faxes on the machine.
4. Retrieve faxes from your fax machine as quickly as possible.

PRIVACY FACTS



Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

SECURITY FACTS

James "Mickey" Kees

Chief Information Officer / HIPAA Security Officer

PUBLIC WI-FI PART 2

As we discussed last month, it may be seldom that you ever need to use a Public Wi-Fi network when performing your work duties. When working remotely, you should be using the LSU VPN (Virtual Private Network) which allows you to communicate private information securely over a public network. But if for some reason you do not have access to a VPN, here are some helpful tips for using public Wi-Fi Networks.

Remember that most Wi-Fi hotspots do NOT encrypt the information you send over the internet, and as a result, are NOT secure. If you use an unsecured network to log in to an unencrypted site – or a site that uses encryption only on the sign-in page – other users will be able to see what you see and what you send. They can hijack your session and log in as you. New hacking tools, available for free online, make this easy, even for users with limited technological knowledge. Your personal information, private documents, contacts, family photos, and even your login credentials could be stolen. A hacker could even test your username and password to try to gain access to other websites, including sites that store your financial information.

You can take the following steps to protect your information when using Wi-Fi. As always, using a VPN is the most secure option.

1. When using a hotspot, log in or send personal information only to websites you know are fully encrypted throughout the entire session – not just at sign in. If you find that you are on an unencrypted page, log out right away.
2. Don't stay permanently signed into accounts. When you have finished using a site, log out.
3. Do not use the same password on multiple websites.
4. Consider changing the settings on your mobile device so that it doesn't automatically connect to nearby Wi-Fi.

Source: Federal Trade Commission

Millions of Patient Records Have Been Compromised

According to an article in FierceHealthIT, IBM is calling 2015 the year of the healthcare security breach. Millions of patient records have been compromised. Healthcare ranks as the top business sector for security incidents, with the following being the largest breaches of the year.

Anthem, Inc. data breach affects 78.8 million – hackers broke into one of the data bases of this insurance carrier, potentially compromising the records stored in its servers.

Premera Blue Cross data breach affects 11 million – similar to the Anthem case, Premera discovered hackers had infiltrated their databases.

Excellus data breach affects 10 million – another insurance company, Excellus discovered it was the victim of a cyber attack dating back as far as December, 2013

UCLA Health System data breach affects 4.5 million - a cyber attack on UCLA that compromised protected data was discovered in May, 2015, though it was first thought that no patient information had been impacted.

Medical Informatics Engineering data breach affects 3.9 million – an electronic medical record vendor learned that it had been a victim of hackers and that the medical records of some of its clients had been compromised.

CareFirst data breach affects 1.1 million – CareFirst, an insurance company announced in May, 2015 that it had been a victim of a cyber attack.

Lesson Learned:

While the largest healthcare breaches all involved cyber attacks, it is important to remember that some of those cyber attacks were successful because employees of the company fell for phishing attacks. A phishing attack occurs when a hacker tries to fool the user into clicking on certain links, websites, or causes the user to give away security information such as passwords. It is important to remember to be suspicious of any requests to give user information or passwords, or to click on links to unsolicited emails!! Cyber criminals will continue their assault on health care organizations due to the value of the information in our data bases if it were to be sold on the black market.

Email Error Leads to Breach of 15,000 Patients' PHI

A physician's office in New York has notified 15,000 patients that a spreadsheet containing their protected health information was emailed out. The physician's office was trying to send out a coupon to its patients. Instead, someone at the office mistakenly attached a spreadsheet that contained patients' Social Security number, names, appointment dates, and home addresses. The office realized the mistake when patients started calling the office stating that they had received the spreadsheet rather than the coupon promised in the subject line of the email.

Lesson Learned:

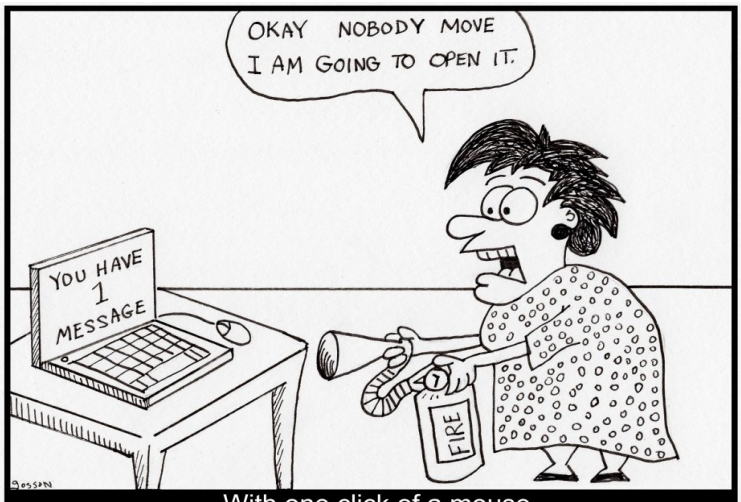
Though difficult to do in the hectic environment of a work day, it is very important to be very cautious when sending emails. Please remember that it is against LSU HCSD and Lallie Kemp Medical Center policy to send any PHI in emails, other than a patient's account number **OR** a medical record number and the patient's initials.

Stolen Laptop Costs Hospital $850,000 in OCR Settlement

Lahey Hospital and Medical Center of Burlington, MA has settled an investigation by the Office for Civil Rights through a costly settlement. The investigation arose from the theft of an unencrypted laptop that was used in conjunction with a portable CT scanner. The laptop was used to operate the CT scanner and record and store medical images via the hospital's Radiology Information System. The laptop was stolen from a treatment room at the hospital. As a result, 599 patient records were compromised. Part of the reason for the large fine was that the hospital failed to put in some basic HIPAA safeguards, such as a unique username and password for each individual accessing the laptop. The laptop was also left in a room unattended and unlocked, making the laptop vulnerable to theft.

Lesson Learned:

It is important to protect patient information no matter where it is stored. All laptops containing patient information must be encrypted, even if the laptop is used to operate diagnostic equipment. Any equipment with patient information must be secured at all times. Access to various equipment and applications should occur through user specific usernames and passwords. If you are aware of any scenarios that places our patients' information at risk, please contact your HIPAA Privacy or HIPAA Security Officer so that we can have the situation corrected.



With one click of a mouse
Suzy exposed the entire office to malware

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