Because We Care, We're HIPAA Aware

HIPAA advisor

HEALTH CARE SERVICES DIVISION

September 2015 Volume 1 Issue 9

Privacy Facts

Do You Know What PHI Is?

You would be surprised how often people forget exactly what PHI is. And if you are not aware of what PHI is, you can violate HIPAA without even realizing it.

Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

A primary function of the HIPAA Privacy regulations is to guard a patient's Protected Health Information (PHI). PHI is any identifier linked to a patient's health information (past, present, or future) that can be directly linked back to the patient.

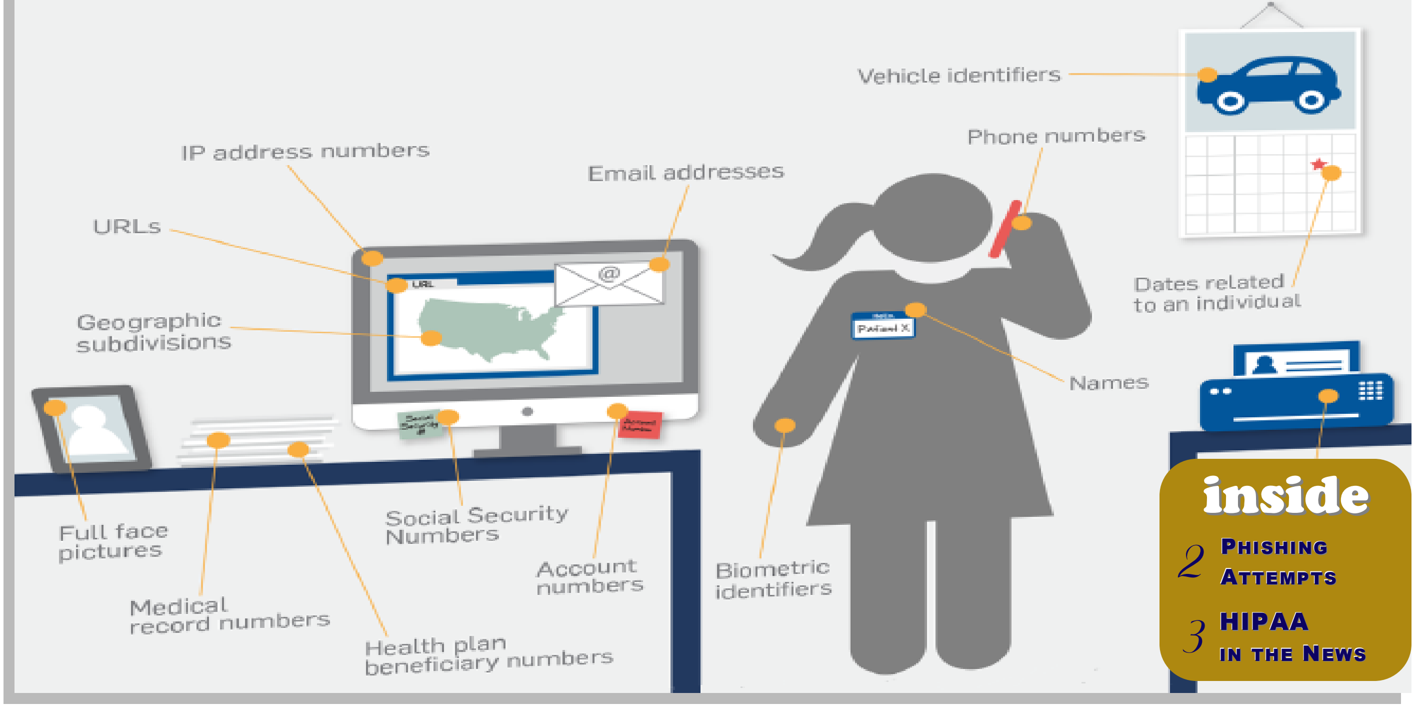
Remember that ANY of these identifiers, whether present on its own or together with other identifiers, must be protected from unauthorized access.

- Patient Name
- Medical Record Number
- Date of Death
- Phone Numbers
- Device Identifiers
- Date of Birth
- Account Number
- Addresses
- Fax Numbers
- Biometric Identifiers
- Social Security Number
- Dates of Service
- Insurance Identification Numbers
- E-Mail Addresses
- Full Face Photographic & Other Comparable Images
- Vehicle Identifiers
- Any Other Identifying Number, Unique Characteristic, or Code

Such information must not be accessible unless there is a specific treatment, payment, or operational **(TPO)** reason to access such information.

We cannot e-mail any such identifiers outside of the LSU E-mail system unless approved. Within the LSU E-Mail system, we can only send Medical Record Numbers **OR** Account Numbers and the patients' initials if used. Please work with I.T. to determine the most secure method. Protect PAPER that may have these identifiers as well. For example, be careful to not place PHI in the regular trash and make sure that you only give patient appointments, discharge papers, etc., to the CORRECT patient by going through EACH piece of paper before turning it over to the patient.

Remember Unsecure PHI Can Be Everywhere... So Be Aware!



Phishing Continues to be a High Risk for Health Care Providers

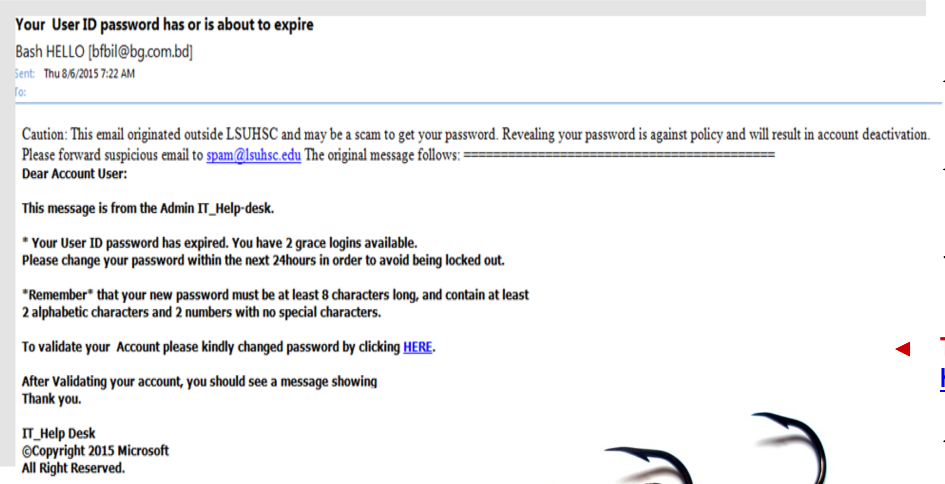
James "Mickey" Kees

Chief Information Officer / HIPAA Security Officer

As we have highlighted before, some of the recent large data breaches in the healthcare and retail industries have been the result of an initial phishing attack. The purpose of phishing is to collect sensitive information with the intention of using that information to gain access to otherwise protected data and networks. One way to protect the LSU system is to help our users recognize what might be a phishing attack.

The following are some examples of recent phishing attempts that were delivered to a LSU HCSD user. Can you spot the phishing attempt and what should alert the user that this is a scam?

Clues this is a phishing attack.....



Your User ID password has or is about to expire

Bash HELLO [bfbil@bg.com.bd]

Sent: Thu 8/6/2015 7:22 AM

To:

Caution: This email originated outside LSUHSC and may be a scam to get your password. Revealing your password is against policy and will result in account deactivation. Please forward suspicious email to spam@lsuhsc.edu The original message follows: ==

Dear Account User:

This message is from the Admin IT_Help-desk.

*** Your User ID password has expired. You have 2 grace logins available.**
Please change your password within the next 24hours in order to avoid being locked out.

***Remember* that your new password must be at least 8 characters long, and contain at least 2 alphabetic characters and 2 numbers with no special characters.**

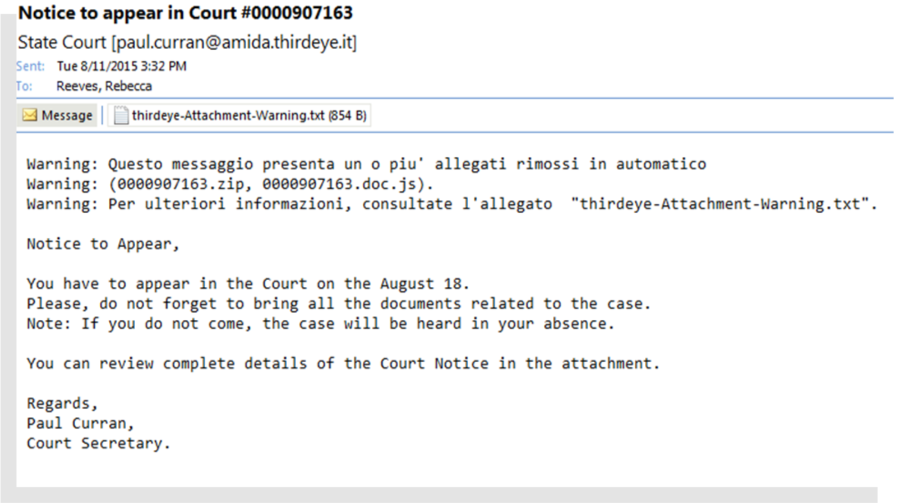
To validate your Account please kindly changed password by clicking HERE.

After Validating your account, you should see a message showing
Thank you.

IT_Help Desk
©Copyright 2015 Microsoft
All Right Reserved.

- ◄ The email address it is originating from is not an LSU address
- ◄ You never get an email saying your password has expired
- ◄ You will never be asked to change your password by clicking HERE
- ◄ **The danger in this email is clicking on the HERE link.**
- ◄ There is a CAUTION at the beginning of the e-mail alerting you that this e-mail comes from outside of the LSU system. But NOTE: You will not always see such a message

How about this one? What should alert you that this is a scam?



Notice to appear in Court #0000907163

State Court [paul.curran@amida.thirdeye.it]

Sent: Tue 8/11/2015 3:32 PM

To: Reeves, Rebecca

```
Warning: Questo messaggio presenta un o piu' allegati rimossi in automatico
Warning: (0000907163.zip, 0000907163.doc.js).
Warning: Per ulteriori informazioni, consultate l'allegato  "thirdeye-Attachment-Warning.txt".

Notice to Appear,

You have to appear in the Court on the August 18.
Please, do not forget to bring all the documents related to the case.
Note: If you do not come, the case will be heard in your absence.

You can review complete details of the Court Notice in the attachment.

Regards,
Paul Curran,
Court Secretary.
```

◄ **The danger in this e-mail is in opening the attachment**

Clues this is a fraud.....

- ◄ A court notice will only come via post-marked mail. It will never come via e-mail.
- ◄ There is no official Court contact information

Electronic Medical Records Company Breach Affects 3.9 Million People

Added to the list of significant healthcare breaches in 2015 is that of Medical Informatics Engineering (MIE) and its subsidiary, NoMoreClipboard. MIE provides an electronic health record product to healthcare providers. MIE discovered suspicious activity in one of its servers on May 26, 2015 and immediately contacted law enforcement in Indiana, where the healthcare providers impacted are based. MIE has determined that up to 3.9 million people within its database may have had their name, phone number, mailing address, Social Security number, security questions and answers, email addresses, birthdates, lab results, diagnoses, and spouse's and children's names and birthdates exposed. Eleven of MIE's healthcare provider customers and 44 radiology centers were affected by the breach in security. The MIE breach is considered particularly dangerous to its victims because of the extensive nature of the personal information compromised. The Indiana State Attorney General has urged all state residents to exercise extreme caution, even going as far as suggesting that residents put a credit freeze on their accounts to protect against identity theft.

Lesson Learned:

Medical Informatics Engineering is a Business Associate of the affected healthcare providers. This incident highlights the importance of completing due diligence with any business associate before signing a contract with them, including a HIPAA Security Risk Assessment. To schedule a HIPAA Security Risk Assessment, contact your HIPAA Security Officer.

Have YOU Been a Victim of Cyber Theft?

Internet Security vendor, iSheriff, recently released the findings of its study that almost 45% of Americans have had their personal information exposed in a healthcare cyber attack. More than 100 million Americans have become victims this year alone, and 143 million have had their information exposed in the last 5 years. Criminals are targeting healthcare due to its relatively low security and high dollar value of the information available. For example, a credit card number that can be stolen from a retail breach is worth only a few dollars on the black market, and credit cards can be quickly cancelled once stolen. However, healthcare data can be used for a longer period of time. And the extent of healthcare data can allow the cyber thieves to do things like file false tax returns, file false insurance claims, secure healthcare services, and take over a person's identity. According to some security experts, it is not a matter of IF you will become a victim of cyber theft, but when. But despite that sobering view, it is important that LSU employees do everything in their power to protect our patients' information. By paying attention to LSU's policies, procedures, and processes, as well as the advice found in this newsletter, you give us all a fighting chance!

Misdirected E-mail Causes Breach of 722 Health Plan Members

UPMC, a Pittsburg, PA health plan notified 722 of its health plan members that their information was accidently emailed to the wrong email address, resulting in their information being compromised. The email was intended for a physician's office, but instead was sent to an incorrect address. The email contained the members' names, member identification numbers, birth dates, phone numbers, and insurance plan type. This is the third time since 2014 that UPMC has had an event that compromised their members' data. UPMC was the victim of hackers in 2014 where 62,000 UPMC employees' data was stolen. In a separate incident later that same year, UPCM had over 2,000 patients' information stolen by an employee of an outside contractor.

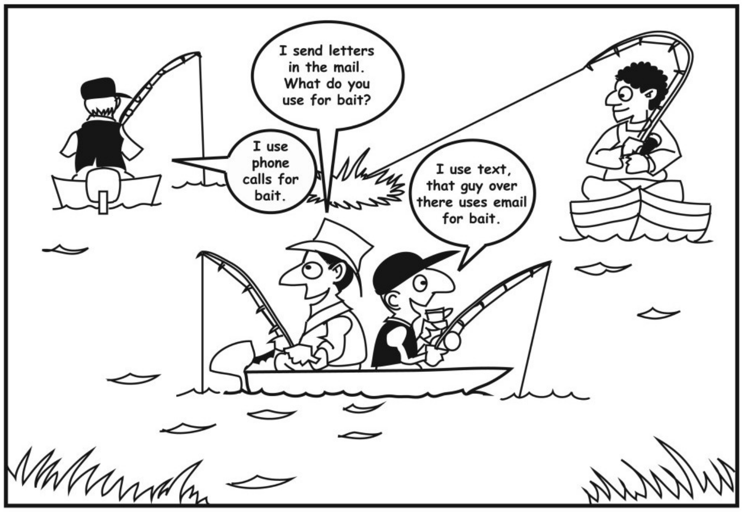
Lesson Learned:

The misdirected email highlights the need to adhere to LSU's policy against including patient information in emails.

Hospital with repeat security failures hit with $218K HIPAA fine

Does your hospital permit employees to use a file-sharing app to store patients' protected health information? Better think again. A Massachusetts hospital is paying up and reevaluating its privacy and security policies after a file-sharing complaint and following a HIPAA breach.

St. Elizabeth's Medical Center in Brighton, Mass. – a member hospital of Steward Health Care system – will pay $218,400 to the Office for Civil Rights for alleged HIPAA violations. The settlement resulted from a 2012 complaint filed by hospital employees, stating that the medical center was using a Web-based document-sharing application to store data containing protected health information. Without adequately analyzing the security risks of this application, it put the PHI of nearly 500 patients at risk.


I send letters in the mail. What do you use for bait?
I use phone calls for bait.
I use text, that guy over there uses email for bait.

"Phishing comes in many forms. Don't take the bait."