Because We Care, We're HIPAA Aware

HIPAA ADVISOR

May / June 2016 | HEALTH CARE SERVICES DIVISION | Volume 2 Issue 3

PRIVACY FACTS

Becky Reeves & Trish Rugeley

Compliance & HIPAA Privacy Officers

OCR Issues Additional Guidance About Patients' Right to Access Health Information

"Providing individuals with easy access to their health information empowers them to be more in control of decisions regarding their health and well-being". – OCR, February 25, 2016.

OCR reiterated that patients have the right to access their health information and PHI, including the right to inspect and/or obtain a copy of that information, as well as to direct the hospital to transmit a copy of the health record to a designated person or entity of the patient's choice. The hospital must ensure that such access is not impeded in any way, though it is important that we all follow the same procedure to ensure that the access meets all of the requirements of the HIPAA Privacy Rule.

Did You Know?

8 in 10 individuals who have viewed their medical record online considered the information useful.

27% of individuals were unaware or didn't believe they had a right to an electronic copy of their medical record.

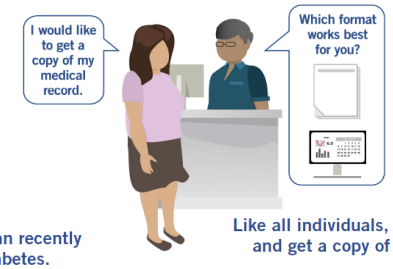
41% of Americans have never even seen their health information.

HIPAA (Health Insurance Portability and Accountability Act of 1996) gives us the right to access our health information.

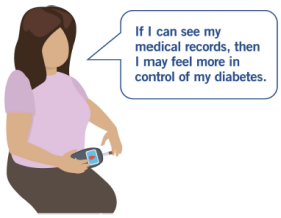
Know Your Rights

You hold the key to your health information and can send or have it sent to anyone you want. Only send your health information to someone you trust.

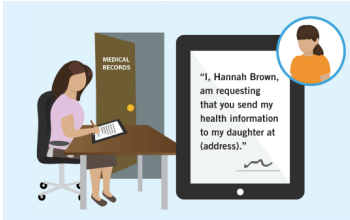
With a copy of your medical record you can become more informed about your health.



Hannah is a 50-year-old woman recently diagnosed with Type 2 Diabetes.



Like all individuals, Hannah has a right to see and get a copy of her health information.



Your provider is no longer responsible for the security of your health information after it is sent to a third party.

Graphics provided by
WWW.HEALTHIT.GOV/ACCESS

To Learn More About Your Rights
ww.hhs.gov/hipaa/for-professionals/privacy/guidance/access

PHISHING ATTEMPTS CONTINUE

ALONG WITH ATTEMPTS TO HIJACK HOSPITAL PATIENT INFORMATION THROUGH RANSOMWARE

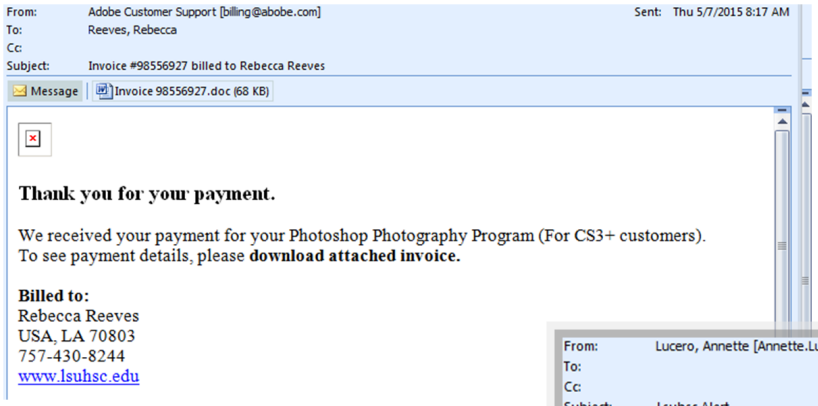
James "Mickey" Kees
Chief Information Officer / HIPAA Security Officer

Hospitals continue to face an increasing threat of phishing attempts and ransomware in 2016.

Since our last HIPAA Advisor publication, the following hospitals announced ransomware attacks:

Methodist Hospital in Henderson, Kentucky
Chino Valley Medical Center and Desert Valley Hospital in Southern California
Alvarado Hospital Medical Center in San Diego, California
King's Daughters' Health in Madison, Indiana
DeKalb Health in Auburn, Indiana
MedStar Health in Columbia, Maryland

LSU HCSD and Lallie Kemp Medical Center are doing what they can to prevent and defend against ransomware attacks. A test system has been launched, issuing phishing emails of our own to see if any of our workforce is vulnerable to a phishing attack. If you happen to fall for one of these test emails, you will be notified and given additional training so that you can better spot phishing attempts in the future. Phishing attempts are becoming much more sophisticated, and so it is understandable that some of our workforce may be tricked into clicking on links in the email.

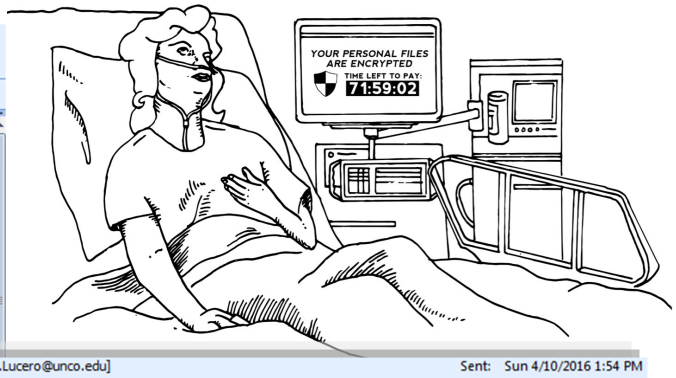


From: Adobe Customer Support [billing@abobe.com] Sent: Thu 5/7/2015 8:17 AM
To: Reeves, Rebecca
Cc:
Subject: Invoice #98556927 billed to Rebecca Reeves
Message | Invoice 98556927.doc (68 KB)

Thank you for your payment.

We received your payment for your Photoshop Photography Program (For CS3+ customers).
To see payment details, please **download attached invoice.**

Billed to:
Rebecca Reeves
USA, LA 70803
757-430-8244
www.lsuhsc.edu



From: Lucero, Annette [Annette.Lucero@unco.edu] Sent: Sun 4/10/2016 1:54 PM
To:
Cc:
Subject: Lsuhsc Alert

EXTERNAL EMAIL: EVALUATE
Lsuhsc Email Online Services.

We would like to point out that we are deleting all old lsuhsc.edu account to create more space for the new account. to prevent your account from been closed, Please click on the link below to update your account:

Click here

Note: Filling of wrong information's will result of closing or suspending your account.

Thank You!

These are some examples of recent phishing attempts to hit LSU HCSD and Lallie Kemp

REMEMBER

WATCH FOR THESE CLUES FOR SUSPICIOUS EMAILS/POP-UPS

Content:

1. Plays on your emotions (fear, greed, urgency, curiosity)
2. Strange text (sometimes poor grammar, misspelled words, unusually formal)
3. Unfamiliar or suspicious email address

Requests:

1. Requires you to click on a link, attachment, or enable macros.
2. Asks for identifying information (user name, password, Social Security #, etc)

WHAT TO DO IF YOU SUSPECT A PHISHING ATTEMPT

1. Do NOT give out any identifying information or click on the email or any link/attachment
2. Do NOT enable macros
3. Call Information Technology IMMEDIATELY

Hospital Is Sued After Compromising Patient Images Caught on Security Cameras

Sharp Grossmont Hospital in San Diego has been sued for breaching the privacy of more than a thousand patients after it took surveillance video in a patient care area.

The hospital was investigating a physician they believed was stealing Propofol from the operating room drug carts. Security cameras were set up in the area. According to the lawsuit, more than 1,000 women had given birth or had medical procedures during the time that the surveillance cameras were in use, all captured on video tape, and studied by security guards at the hospital as part of the investigation into the alleged drug theft. Some of the video was also shared with the physician's attorney, who advised the hospital that fourteen of the video clips he had been given to review contained images of patients undergoing procedures.

Lesson Learned:

It is important to carefully think through any circumstance where patient information is going to be exposed to ensure that our patients' confidentiality is protected.

Stolen Logbook Potentially Exposes Patient Information

An emergency medicine physician group reported the potential breach of approximately 1,000 individuals after a physician's log book was reported stolen from the physician's vehicle. The hand written log book contained information such as patient names, dates of birth, ages, genders, dates of service, medical record numbers, and descriptions of medical issues. The group, Emergency Medicine Associates, stated that while there was no policy against such logbooks at the time of the theft, they have reviewed and revised their policies regarding logbooks and provided additional training to its physicians to try to avoid similar events in the future.

Lesson Learned:

Practitioner logbooks are not an uncommon practice, but it is a practice that puts a large amount of patient information at risk since PHI on paper is so vulnerable to loss and theft. Practitioners must be very cautious when using such logbooks, and ensure that the information is protected against loss and theft, much like you would a laptop. Logbooks are not a recommended practice, but if used, extreme caution must be taken to ensure that the PHI contained within is protected within and outside of the hospital.

Former Respiratory Therapist Convicted of Unlawfully Obtaining Computerized PHI

A former employee of ProMedica Bay Park Hospital in Oregon, Ohio was convicted June 23, 2016 of accessing the PHI of 596 hospital patients for purposes of seeking, obtaining, or using intravenous drugs. While the employee had access to the hospital's electronic health record in order to provide respiratory care to the hospital's patients, the therapist also used that access to gain patient information not related to the care she was providing.

When the unauthorized access was originally discovered, the hospital declined to file charges against the former employee. However, the federal authorities chose to pursue the case, and were successful in prosecution. Sentencing will occur later this year.

Lesson Learned:

Patient information may only be accessed for the purpose of performing your job function. While a variety of life's circumstances may make it tempting to access PHI for personal reasons, some benevolent and others not, it is never acceptable to use our patient's PHI for personal purposes. While cases of criminal prosecution for HIPAA violations are rare, they do happen.

Hacker Lists 655,000 Medical Records for Sale

A hacker calling himself "TheDarkOverlord" claims that he stole medical records in three separate cyberattacks on hospitals throughout the United States, and is now selling them for a Bitcoin equivalent of $682,110. The same hacker claims to have already sold a group of Blue Cross/Blue Shield members' data for $100,000. The stolen data includes patients' names, addresses, dates of birth, email addresses, and Social Security numbers. This data is valuable to criminals who want to commit identity theft. The hacker states he stole the data by exploiting Remote Desktop Protocol, or RDP. RDP is used by vendors to remotely access hospital computer systems to assist hospitals in updating or repairing computer system issues. The hacker also promises that there is a "lot more to come", indicating that there is data still at risk for going up for sale. Even more frightening is the fact that the data breaches that the hacker references have not yet been reported, which causes one to wonder if the healthcare organizations may not be aware that their data has been hacked.

Lesson Learned:

It is vital that healthcare organizations strive for the tightest security possible for each of its systems, in each of their forms. Healthcare data is under attack more today than ever before, and every workforce member needs to view computer security as a top priority. Our patients' identity security depends on it!

"Follow proper health records disposal policies!"

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