Issue 3, Winter 2016

This newsletter is prepared by the Office of Compliance and is intended to provide you with current information about HIPAA and other privacy issues. For additional information, to view past newsletters, or to provide comments about this or any future issues of this newsletter, please contact the Office of Compliance at (213) 740-8258 or at compliance@usc.edu.

The Office for Civil Rights (OCR) Announces Three New Settlements of HIPAA Violations

OCR ended 2015 with a flurry of activity, announcing three new resolution agreements to settle claims of HIPAA violations. Massachusetts-based Lahey Hospital and Medical Center will pay $850,000 for violations uncovered after a breach of a medical device; University of Washington Medicine will pay $750,000 after an investigation of a breach caused by an employee's downloading of an email attachment that contained malware and compromised patient records; and insurance plan Triple S Management Corp. will pay $3.5 million after incurring "multiple" breaches. All of the settlements involve situations where the health care entity was out of compliance with HIPAA, including failure to conduct risk analyses of vulnerabilities of electronic patient health information, lack of policies and procedures and lack of security safeguards, such as poor protection of data at workstations.

HHS offers tips on how to protect and secure health information when using mobile devices: https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

The Lahey Resolution Agreement and Corrective Action Plan can be found on the OCR website. And to learn more about the other settlements, go to http://www.hhs.gov/hipaa/newsroom/index.html.

Source: Medical Practice Compliance Alert

"Hey, Can You Hold That Door Open?" and Social Engineering Attacks

Social engineering is the art of obtaining information through deceptive methods. A common social engineering tactic to gain access to certain buildings or secure workspaces is tailgating or piggybacking. This type of attack occurs when a person who lacks the proper authorization (e.g. an access badge) uses deception to gain access into sensitive areas of a workplace.

Would-be tailgaters might strike up a conversation with you to create just that sense of familiarity needed to catch you off guard, to get past weak or busy access controls like reception desks, or to circumvent badge access readers.

The common courtesy of holding doors open for others does not apply to entry into secure and non-public areas of the workplace. The risks of

The USC Help & Hotline is a number that all faculty, staff, and students can use to report suspected violations of an applicable law, regulation, or university policy confidentially and without fear of retribution. The Help & Hotline can also be used to ask questions about applicable laws, regulations, and university policies that may impact your job duties.

*The USC Help & Hotline is staffed 24 hours a day, 365 days a year: (213) 740-2500 or file on the web and enter **UOSC** as the access code.*

tailgating into sensitive areas include: theft of equipment, theft of patient, employee, and other sensitive information, workplace violence, and even attacks on our network. If we don't see tailgating as a problem, there is also a risk we might be overlooking other security risks.

It's possible both to be nice and to promote good security. To reduce the risks that can come with tailgating, follow these best practices:

- Wear your USC/hospital ID badge above the waist at all times so your picture, name, and department are clearly visible to others.
- Remind work colleagues to wear their badges if they forget.
- If you see someone without a badge in a non-public area of your building, stop, ask the person how you can help them, then escort them to the reception/information desk. If the person is uncooperative, call security.
- If an access door requires a badge for entry, never hold the door open unless you can identify the person behind you and know they are authorized entry.
- Never prop open a door to a secure or non-public area

And remember, if someone gets a bit grouchy because they forgot their badge or have to walk around to a public entrance, it's ok. You did the right thing!

For information on other social engineering tactics, see: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_en.pdf

How To Secure Text Messages in the Electronic Healthcare Environment

Texting has become an increasingly common form of professionally acceptable communication. According to Bloomberg Big Number, eight-trillion text messages are sent every year. And while text messaging has significant benefits, many healthcare providers do not recognize the privacy, security, and malpractice risks posed by text messaging. These risks can be mitigated through the application of technology and proper policies and procedures.

Text messaging in the healthcare context not only raises privacy and security issues, but also raises additional concerns with respect to record keeping requirements of patient medical information and possible malpractice risks. Text messaging does not comply with the security regulations under the Health Information Portability and Accountability Act (HIPAA). If a physician is utilizing a text messaging service, the physician and healthcare facility may need to consider entering into a Business Associate Agreement with the entity providing the text messaging service. Once the phone is stolen or misplaced, HIPAA's breach notification requirements are triggered. Failure to properly comply with federal or state breach notification laws can lead to significant financial penalties on a covered entity. While texting is beneficial for ease of communication, texting may inadvertently create privacy and security related risks.

To protect patient privacy, recommendations for using texting include:

- limiting the type and amount of PHI sent and received;
- stringent password policies;
- phone encryption;
- proper disposable and recycling methods of your mobile device;
- use of secure HIPAA-compliant text messaging and a clinical

communications vendor, which has a SOC 2 report

For clinical faculty and personnel at Keck, please also refer to "Minimum Security Standards for Electronic Protected Health Information for Keck Medicine." Providers also should use encourage patient use of the Keck Portal to communicate electronically with patients at http://myuscchart.keckmedicine.org/.

To read the full article, please visit:
https://iapp.org/news/a/how-to-secure-text-messages-in-the-electronic-healthcare-environment/

Who Else Has Accessed Your Medical Data?

The UCLA Health system's computer network suffered a cyberattack affecting the personal information of as many as 4.5 million people. Data breaches like the one UCLA Health experienced are a growing problem. These breaches typically disclose sensitive personal information, including Social Security numbers, dates of birth and data about patients' health insurance and other medical information.

The biggest concern for consumers whose health information has been stolen, experts say, is medical identity theft - when criminals with access to health insurance information & use it to seek care and rack up medical bills in your name.

Though medical identity theft cannot be completely prevented, experts suggest steps to help minimize your risks.

- ***Share information sparingly.*** Patients are routinely asked to share their Social Security numbers when seeing a healthcare provider for the first time. But it's not required to deliver care.
- ***Sign up for monitoring services.*** Credit monitoring is a common offering after data breaches, and something experts say consumers should take advantage of. Once you do, actively monitor the reports.
- ***"Freeze" out the criminals***. Stephens points out that identity protection tools, while helpful, notify you only if something has happened after the fact.
  A better approach, he says, is to place a security freeze with all three credit firms (Equifax, Experian and TransUnion).

For the full article, please visit:
http://www.latimes.com/business/la-fi-healthcare-watch-20150821-story.html