Issue 4, Winter 2017

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.

UMass Amherst Hit with $650,000 HIPAA Settlement

In November, federal regulators have slapped the University of Massachusetts Amherst with a $650,000 financial settlement and corrective action plan after investigating a 2013 breach involving a malware infection at a campus speech and language center.

OCR in its statement says that on June 18, 2013, UMass reported that a workstation in its Center for Language, Speech, and Hearing was infected with malware, resulting in the impermissible disclosure of electronic protected health information of 1,670 individuals, including names, addresses, Social Security numbers, dates of birth, health insurance information, diagnoses and procedure codes.

OCR says its breach investigation found the following potential violations of HIPAA:

- While UMass correctly identified that its University Health Services was a HIPAA-covered healthcare component, it failed to designate the center where the breach of ePHI occurred as a HIPAA-covered component, and thus "did not implement policies and procedures at the center to ensure compliance with the HIPAA privacy and security rules."
- UMass failed to implement technical security measures at the speech and language center to guard against unauthorized access to ePHI transmitted over an electronic communications network by ensuring that firewalls were in place.
- UMass did not conduct an accurate and thorough risk analysis until September 2015.

Read the fill article here: http://www.databreachtoday.com/umass-amherst-hit-650000-hipaa-settlement-a-9554

HIPAA Settlement Illustrates the Importance of Reviewing and Updating, as necessary, Business Associate Agreements

On September 23, 2016, the U.S. Department of Health and Human Services (HHS) announced a $400,000 settlement and corrective action plan with Care New England Health System (CNE) for potential violations of the HIPAA privacy and security regulations. CNE, a business associate to a hospital facility, lost unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals, including patient name, data of birth, date of exam, physician names, and, in some instances Social Security Numbers. While the parties had a business associate agreement, it had not been updated to incorporate revisions to the privacy rule.

This case illustrates that not only must business associate agreements be in place, but they must be updated to incorporate HITECH provisions. When negotiating agreements with business associates, please make sure to use USC's template BAA, which incorporates HITECH's provisions.

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.*

Read the full article here:
http://www.hhs.gov/about/news/2016/09/23/hipaa-settlement-illustrates-importance-of-reviewing-updating-business-associate-agreements.html

And you can find USC's policy on Business Associates (BUS-701) here: http://policy.usc.edu/hipaa/

Yes, Staff Snooping of Medical Records is a Privacy Breach

Medical Economics reported, "A privacy breach can come in many forms. Breaches due to ransomware attacks have been grabbing headlines recently, and with good reason: the FBI estimates there are now an average of 4,000 attacks daily in the United States. But there are many other, even more common, types of privacy breaches which can be both embarrassing and potentially expensive for medical practices.

For example, if someone on the staff sees a neighbor come into the office and, out of curiosity, checks the patient's record to see why they are seeing a doctor, it is considered snooping and constitutes a breach of privacy. Another example is if something happens in the community, such as a car accident or shooting, and someone looks at patient records after watching the news to find out what happened.

Although such incidents may seem harmless, they still constitute privacy breaches, and carry all the same risks."

Read the full article here:
http://medicaleconomics.modernmedicine.com/medical-economics/news/yes-staff-snooping-medical-records-privacy-breach

Report Warns of Potential HIPAA Violations When Providers Respond to Negative Online Reviews

ProPublica, a public interest investigative newsroom, recently identified more than 3,500 one-star medical reviews on Yelp in which patients complained about privacy issues. For example, ProPublica noted consumers giving providers negative reviews on Yelp and providers responding with details about the "patients' diagnoses, treatments and idiosyncrasies."

As more and more patients use online review platforms to select their providers, many providers are paying close attention to reviews. However, providers need to balance their business concerns with their HIPAA compliance obligations when responding to negative reviews. Note that disclosure by the patient of their own PHI does not constitute a waiver of the privacy right. A covered entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule. A patient disclosing their health information does not constitute the necessary authorization needed for the provider to disclose the information.

What are some practical solutions? A provider may legally respond to reviews in a number of ways:

1. Increase positive reviews instead of responding to negative ones
2. Respond with a general treatment philosophy
3. Treat the conflict offline

The U.S. Department of Health and Human Services Office of Civil Rights enforces HIPAA and may impose significant fines for each violation.

Read the full article here:
https://www.healthcarelawtoday.com/2016/07/25/4561/

Health Apps and HIPAA: OCR Publishes New Privacy Guidance for Health App Developers

In response to requests from developers of mobile health applications, the Department of Health and Human Services Office for Civil Rights ("OCR") released a new guidance document addressing the applicability of HIPAA to applications that collect, store or transmit health information. The guidance document, entitled "Health App Use Scenarios & HIPAA" ("Health App Guidance"), sets forth several factual scenarios involving mobile health apps, along with OCR's explanation of whether, in each scenario, HIPAA would apply to the developer of the application.

The Health App Guidance also clarifies that a health app that is downloaded and used solely by individual consumers does not result in the app developer's becoming subject to HIPAA. The reason for this result is that the developer is not creating, receiving, maintaining or transmitting PHI on behalf of a CE or BA. On the contrary, the PHI being used or stored by the app is directly from, and for, the consumer.

However, a developer who contracts directly with a CE to collect, maintain or transmit PHI through a particular health app is deemed to be a BA under HIPAA, and accordingly will be subject to HIPAA requirements because the developer is providing a service for the benefit of the CE and has access to the PHI of the CE. A developer who contracts with a BA on behalf of a CE to do the same thing likewise will be subject to HIPAA.

The Health App Guidance concludes with a series of questions that developers should consider about their business and their health apps to determine if they are BAs.

You can find the OCR guidance: http://www.hhs.gov/blog/2016/02/11/ocr-adds-new-health-app-use-scenarios-to-developer-portal.html