Having trouble viewing this email?Click here

Please add complian@usc.edu to your address book so we'll be sure to land in your inbox.

You may unsubscribe if you no longer wish to receive our emails.

USC Office of Compliance

PRIVACY NEWSLETTER

Issue 1, Spring 2015

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 complian@usc.edu.

Welcome to the First Issue of the USC Privacy Newsletter!

The Office of Compliance has created this separate newsletter to focus on current issues and trends regarding privacy and security of health and other sensitive information.

We hope that you find it informative and helpful.

The Anthem Breach

In late January 2015, Anthem Blue Cross disclosed a major breach of its information systems, which may have resulted in the unauthorized access of current and former enrollee personal information, including member name, date of birth, Social Security number, member ID, address, and email address.

USC contracts with Anthem for parts of our university-sponsored medical benefits. The administration of these benefits requires Anthem to maintain certain personal information to confirm eligibility for those individuals enrolled in any Anthem plan or the USC Network Medical Plan. USC faculty and staff who are enrolled in the USC Network Plan, Anthem MyChoice PPO, or the Anthem HMO plans may be impacted by this breach.

Anthem is offering 24 months of identity repair assistance, credit monitoring services, and identity theft insurance to all current and former members of affected Anthem plans dating back to 2004. These services are available now and are free of charge. Identity repair assistance is offered automatically and no enrollment is necessary. To receive free credit monitoring services and identity theft insurance, members need to enroll at https://anthem.allclearid.com or call 1-887-263-7995 for assistance. Impacted members will receive notification letters in the mail.

For more information about the Anthem data breach, you can visit www.AnthemFacts.com.

Spotlight on Protecting Electronic PHI ("ePHI")

With the rise of the use and release of electronic health information (ePHI), now more than ever, it is everyone's responsibility to do their part in securing ePHI. Here are some basic precautions that all clinicians, staff, and administrators can take when using ePHI:

- Use email systems with encryption (like the "MED" email system) when transmitting health information electronically. If your email system does not have email encryption technology, do not send ePHI electronically.
- Make sure that your laptop and removable media (e.g., USB drive) are encrypted before you use it to store or send ePHI.
- Report any lost or stolen devices immediately your school IT department;
- Secure your passwords and do not share with others;
- Do not send ePHI via text message;
- Log off your work station at the end of the day;
- Use caution in selecting the correct "cc" on an email containing PHI;
- Use caution in selecting the right patient name or medical record number while working in a record;
- Do not access a patient's chart without a valid reason - even if you have been granted the authority to access patients' records as part of your job responsibilities, this does not mean that access applies to any patient chart.
- For clinicians at Keck Medical Center, use the Keckcare patient portal when communicating with patients;
- For the clinicians at Keck Medical Center, follow the minimum security standards for ePHI at: http://policy.usc.edu/files/2014/02/CLIN-206-Minimum-Security-Standards-for-ePHI-for-Keck.pdf

Remember to immediately report any potential breach or security incident to the Office of Compliance.

Lack of Encryption Leads to HIPAA Breach for 45,000 Patients in Indiana

Approximately 45,000 people are receiving HIPAA breach notification letters after a mental health provider failed to encrypt laptops containing clients' medical data and Social Security numbers.

Aspire Indiana, a mental health organization located in central Indiana, has notified 45,030 of its clients and employees after several unencrypted laptops were stolen from its administrative office last fall.

Following an investigation of the incident, Aspire officials determined emails on the laptops contained client and employees' Social Security numbers, names, and addresses. 1,548 of those notified had their Social Security numbers compromised. The laptops also contained personal health information of Aspire clients. Health information Aspire collects includes HIV care data, substance abuse treatment, and mental health services.

For more information, please visit: http://www.healthcareitnews.com/news/no-encryption-means-hipaa-breach-45k

Changes to California HIPAA Reporting Requirements

Effective January 1, 2015, licensed health facilities will have fifteen (15) business days to investigate and report violations of the California Medical Information Act (CMIA). Prior to the change in the law, licensed health facilities had only five business days to report such violations.

This new reporting period is still much shorter than the time to report a breach under HIPAA. Please make sure to contact the Office of Compliance immediately if you suspect an actual or potential breach. Failure to report unlawful or unauthorized access within the 15-day period can result in a penalty of $100 for each day the unlawful or unauthorized access, use, or disclosure is not reported to the CDPH or the affected patient up to $250,000 per reported event.

For more information, please visit:
http://www.lexology.com/library/detail.aspx?g=2e179f7c-2f47-4a89-8883-80d5fac42cfd

OCR Audit Delay Enforcement Ramp-Up

The Department of Health and Human Services' Office for Civil Rights ("OCR") announced that it would delay its next phase of federal HIPAA compliance audit, which was supposed to begin last Fall 2014. No timeline has been announced, but OCR appears intent on continuing the audit process.

While this initially was couched as an educational initiative, it appears that OCR may begin to use the audit findings as a tool for enforcement. Security deficiencies, including lack of encryption and appropriate safeguards, continue to be some of the more common audit findings.

USC continues to work with potentially impacted clinical units to prepare for a potential HIPAA audit. Please contact the Office of Compliance if you wish to participate in this effort.

Forward this email

SafeUnsubscribe

This email was sent to thawthorne@ooc.usc.edu by complian@usc.edu |
Update Profile/Email Address | Rapid removal with SafeUnsubscribe™ | Privacy Policy.

Trusted Email from Constant Contact FREE
Try it FREE today.

USC Office of Compliance | University Gardens Building | 3500 S. Figueroa Street | Suite 105 | Los Angeles | CA | 90089-8007