December | 2015

Compliance for you

DECEMBER NEWSLETTER EDITION

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

Office *of* Institutional Compliance

TTUHSC Safe Campus Commitment – Title IX

Members of the TTUHSC community of students, faculty and staff, guests and visitors have the right to be free from all forms of sex/gender harassment, discrimination and misconduct, examples of which can include acts of sexual violence, sexual harassment, domestic violence, dating violence, and stalking. All members of the campus community are expected to conduct themselves in a manner that does not infringe upon the rights of others. TTUHSC is committed to providing a positive and safe learning, teaching and working environment for our community. To ensure this commitment, students, faculty and staff are expected to complete annual Title IX Mandated Reporter Training required training and review the information provided on the TTUHSC Title IX website.

WHAT IS TITLE IX?

Title IX of the Education Amendments of 1972 (Title IX) prohibits discrimination on the basis of sex in any federally funded education program or activity. Federal law specifically states that: ***"No person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any educational program or activity receiving federal financial assistance."*** **Education Amendments of 1972.** Title IX protects students, employees (faculty and staff), applicants for admission and employment, and other persons from all forms of sexual discrimination. Sexual harassment, which includes sexual violence, is a form of sex discrimination.

WHO HAS THE RESPONSIBILITY TO REPORT? Any member of the university community (students, faculty and staff) are responsible for reporting immediately any Prohibited Acts they experience, witness or which are communicated to them. Licensed professional counselors and staff, medical providers, related off-campus resource centers and professionals or clergy do not have a responsibility to report. Furthermore, any member of the university community who becomes aware of possible sexual harassment or sexual assault perpetrated by a TTUHSC employee or student, not acting within the scope of their employment or educational program, should promptly contact the Title IX Coordinator to discuss the matter.

WHO TO CALL?

Title IX Coordinator	**Students**	**Faculty and Staff**
Dr. Gena Jones, Assistant Vice President for Human Resources TitleIXCoordinator@ttuhsc.edu 806 743-2865	Margret Duran Assistant Vice President of Student Services, Deputy, Title IX Coordinator TitleIXCoordinator@ttuhsc.edu 806 743-6426 Receives complaints of sexual harassment, including sexual assault, sexual violence or other sexual misconduct, against students.	Charlotte Bingham Assistant Vice Chancellor Admin/ Director EEO Deputy, Title IX Coordinator TitleIXCoordinator@ttuhsc.edu 806 834-2713 Receives complaints of sexual harassment, including sexual assault, sexual violence or other sexual misconduct, against faculty and staff.

Question: What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?

Answer:
Covered entities must:

- Implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information.
- Implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored
- Implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.
- Ensure that workforce members (including volunteers) receive training on and follow the disposal policies and procedures of the covered entity.
- Covered entities are not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons.

The Privacy and Security Rules do not require a particular disposal method. Examples of proper disposal methods may include, but are not limited to:

- For PHI in paper records suggested disposal methods are: shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

For more information on proper disposal of electronic PHI, see the HHS HIPAA Security Series 3: Security Standards – Physical Safeguards. In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult NIST SP 800-88, Guidelines for Media Sanitization.

Question: What does the HIPAA Privacy Rule do?

ANSWER: Most health plans and health care providers that are covered by the new Rule must comply with the new requirements by April 14, 2003.

The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information. It gives patients more control over their health information. It sets boundaries on the use and release of health records. It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information. It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights. And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used. It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made. It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure. It generally gives patients the right to examine and obtain a copy of their own health records and request corrections. It empowers individuals to control certain uses and disclosures of their health information.

Top Ten Things You Should Know About Data Breaches

2014 was dubbed as 'the year of the data breach'. With many new data breaches dominating the headlines in 2015, including **Anthem**, the **White House**, banking attacks, and the latest **employee data theft at the US federal government**, one can only imagine what the name for 2015 will be: the year of even more data breaches? According to the **Ponemon Institute**, 43% of companies experienced a data breach in 2014. Not only is the number of data breaches rising, the number of records stolen per breach is increasing as well as the cost per stolen record. It is apparent that current security measures are not sufficient to protect organizations from data breaches.

The SANS Institute reports that a whopping 95% of all attacks on enterprise networks gained entry through a **spear phishing attack**. A spear phishing attack is an email targeted at specific individuals that are engineered to look legitimate and fool even tech-savvy users. The email has a malicious attachment or link that when opened installs malware and tries to gain system access. Clearly, spear phishing attempts are sometimes able to get past traditional spam filters and antivirus engines. No single antivirus engine will be able to block every threat. However, by deploying **multi-scanning** with multiple antivirus engines, the different detection algorithms and heuristics of each engine can be combined, which significantly increases the malware detection rate for known and unknown malware. Other technologies such as data sanitization and file type verification can also prevent threats that may go undetected by antivirus engines.

Below, we have highlighted the top 10 most interesting, remarkable, and troubling facts about data breaches:

The number of stolen records went up 78% in 2014
According to the 2014 Breach Level Index by Gemalto, one billion records were compromised in 2014 in more than 1,500 data breaches; a 78% increase compared to 2013.

Cost of data breach rose 23% since 2013
The total cost of a data breach increased 23% since 2013, as reported in the Ponemon Institute's Annual Cost of Data Breach Study. In 2015 the average cost per lost or stolen record is $154.

The most costly breaches were in US and Germany
The Ponemon Institute reports that the most costly breaches are in the US ($217 per record stolen) and Germany ($211 per record stolen).

The healthcare sector had the highest cost per stolen record
The cost of stolen healthcare records can be as high as $363, according to the Ponemon Institute. Healthcare records are more valuable than stolen credit card details since credit cards can easily be cancelled, but fraud using a person's medical records is much more difficult to stop.

Identity theft was the most common motive
Gemalto's research shows that the majority of data breaches are now perpetrated for the purpose of identity theft rather than stealing credit card information. In 2014, 54% of data breaches were motivated by identity theft, compared to 20% in 2013. In 2014 only 17% of data breaches were for financial access, down from 50% in 2013.

Malicious outsiders are behind a majority of attacks
The 2014 Breach Level Index by Gemalto reports that 55% of the data breaches were perpetrated by malicious outsiders, 25% were due to accidental loss, and 15% were committed by malicious insiders.

95% of breaches start with phishing attack
According to Allen Paller, director of research at the SANS Institute, 95% of all attacks on enterprise networks gained entry through a spear phishing attack. A spear phishing attack is an email targeted at specific individuals that is engineered to look legitimate and fool even tech-savvy users. The email either has a malware-laced attachment or a malicious link that when opened installs malware and tries to gain system access.

Traditional spam filters cannot detect spear phishing attacks
Most spam filtering products detect spam by checking black lists and known spam. However spear phishing emails are composed with considerable effort and target only a small number of individuals, therefore staying under the radar of traditional spam filters.

A single anti-virus engine is not enough to protect against all threats
With 450,000 new threats emerging daily, a single anti-virus solution is no longer going to cut it. By scanning email attachments and web content with multiple antimalware engines you are multiplying the chance that known as well as unknown malware is detected, speeding up protection against outbreaks, and protecting against threats designed to exploit vulnerabilities in specific engines.

It's a question is not if, but when
Data breaches are becoming more prevalent and more sophisticated. Suffering a breach is no longer a question of if but when. It is important that companies start increasing their security defenses.

*Sourced from Deborah Galea, manager, **OPSWAT***

The relationship between the *Family Education Rights and Privacy Act* (*FERPA*) and the *Health Insurance Portability and Accountability Act of*

FERPA HIPAA

Have you ever wondered which law applies to student health records? Generally, FERPA, not HIPAA, applies to all student health records maintained by a college or university student health care center. These records are either considered "education records" or covered "treatment records" but it is not "protected health information". Student health records cannot be disclosed to faculty, staff, or third parties without the student's prior written consent. It is important to note that any treatment records maintained by the clinic for **non-students** (i.e. faculty, staff, and family members) are not covered by FERPA and are covered by HIPAA.

- ***FERPA*** is a Federal law that protects the privacy of students' "education records." (See 20 *U.S.C.* § 1232g; 34 *CFR* Part 99). *FERPA* applies to educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education.

- ***HIPAA*** requires covered entities (health plans, health care clearinghouses and health care providers) to protect individuals' health records and other identifiable health information by requiring appropriate safeguards to protect privacy, and setting limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

Keep in mind that a student's health record, including immunization information and other records maintained by a school nurse/student health care center are considered part of the student's education record and are protected from disclosure under *FERPA*. Disclosure exceptions under *FERPA* are limited in order to protect the student's privacy.

This is just a couple of key points and examples regarding FERPA and HIPAA. For more details and other helpful information go to http://www.hhs.gov.

UCLA Health Notifying Patients of Stolen Laptop Containing Personal Health

UCLA Health is sending notification letters to 1,242 individuals about the theft of a laptop computer containing patient names, medical record numbers, and health information used to help prepare patient treatment plans. The laptop, which was password protected but **not encrypted**, was reported stolen and belonged to a UCLA faculty member.

According to an OCR spokesperson, lost and stolen unencrypted computing devices have been involved in 57 percent of the 1,310 major HIPAA breaches reported to the Office for Civil Rights from September 2009 to August 28, 2015.

Important Note: The best defense for avoiding a HIPAA breach is to have your laptop or other mobile devices encrypted! Please contact IT security for information on how to encrypt your mobile devices. 806-743-1234 .

TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER
Office of Institutional Compliance

www.ethicspoints.com

1.866.294.9352

www.ttuhsc.edu/compliance
806.743.3949