○ September | ○ 2016

Compliance *Newsletter*

HIPAA Privacy and Security Special Edition: Cyber-Awareness

The Office for Civil Rights (OCR) at the Department of Health and Human Services announced the launch of a cyber-awareness initiative for the healthcare industry on February 2, 2016. OCR has been sending out monthly updates to its regulated communities to help them become more knowledgeable about the various security threats and vulnerabilities that currently exist in the healthcare sector; what security measures can be taken to decrease the possibility of being exposed by these threats; and how to reduce breaches of electronic protected health information (ePHI).

Healthcare Data Continues to Be What Hackers Target

According to this year's 6th Annual Benchmark Study on Privacy & Security of Healthcare Data, data breaches in healthcare are consistently high in terms of volume, frequency, impact, and cost for the sixth year in a row. About 90 percent of healthcare organizations had a data breach in the past two years, and almost half of them had more than five data breaches in the same time period.

Once again, criminal attacks are the leading cause of half of all data breaches in healthcare, a five-percent increase from last year's study. According to OCR, criminals now are finding new ways to monetize health information. Personal health information may be stolen and sold to the uninsured, used to get medical supplies and equipment that can be sold, or used to submit fake insurance claims. Employee mistakes, third-party snafus, and stolen computer devices—are the root cause of the other half of data breaches.

In this special edition: HIPAA Privacy and Security: Cyber-Awareness, we are going to introduce several of the latest threats and tools that may be available regarding ePHI and healthcare breaches, selected from OCR's Cyber-Awareness monthly updates.

Prepare for Thousands of ICD-10 Changes

It's final that more than 3,000 ICD-10-CM code changes are coming. The updates will impact specifically OB/GYN, primary care, and Orthopedic practices.

Review the new ICD-10-CM guidelines. The guidelines, which the Centers for Disease Control (CDC) posted on its website on Aug. 5, are the final piece of the first ICD-10-CM update in five years. New and revised information is scattered through all three subsections of section 1, and include changes to the guidelines for 10 chapters.

The AAPC webinar for ICD-10-CM 2017 updates is also available on Sept. 28, 2016 for you to view. For more information or resources, please contact Sylvia Riojas at sylvia.riojas@ttuhsc.edu.

New Cyber Threats and Attacks on Healthcare

Ransomware

Ransomware is malicious software that locks computer files with encryption, preventing the authorized users from accessing their data. A security key must be used to decrypt locked data. That security key is held by the attackers, and is only released when a ransom is paid. Ransomware is infected through a number of vectors, such as email attachments, MMS text messages, botnets, malvertising, hijacked websites, and malicious websites containing exploit kits.

In healthcare, the main objective in using ransomware is to destroy backups of files and databases that contain ePHI and to lock up files and databases in order to charge covered entities and business associates hundreds to thousands of dollars to unlock the data. To combat ransomware infections, OCR recommends that we:

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process.
- Maintain up-to-date anti-virus software.
- Keep operating system and software up-to-date with the latest patches.
- Not follow unsolicited web links in emails.

  ***Never give your password to anyone.**
- Use caution when opening email attachments.
- Follow safe practices when browsing the web.

Smartphone Attacks

Patients, staff, and third-parties of covered entities are using smartphones to interact with new healthcare applications and medical devices.

Although smartphones have beneficial features, entities must ensure these devices have appropriate safeguards against cyberattacks. To reduce cyberattacks on smartphones:

- Consider its security features, when choosing a mobile phone
- Configure the device to be more secure. Enable the password feature on mobile phone and choose a reasonably complex password.
- Do not follow links sent in a suspicious email or text messages.
- Limit exposure of your mobile phone number.
- Carefully consider what information you want to store on the device.
- Be choosy and do a little research on mobile applications before installing them.
- Maintain physical control of the devices in public or semi-public places.
- Disable interfaces that are not currently in use, such as Bluetooth, infrared, or Wi-Fi.
- Set Bluetooth-enabled devices to non-discoverable.
- Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots.
- Delete all information stored in a device prior to discarding it.

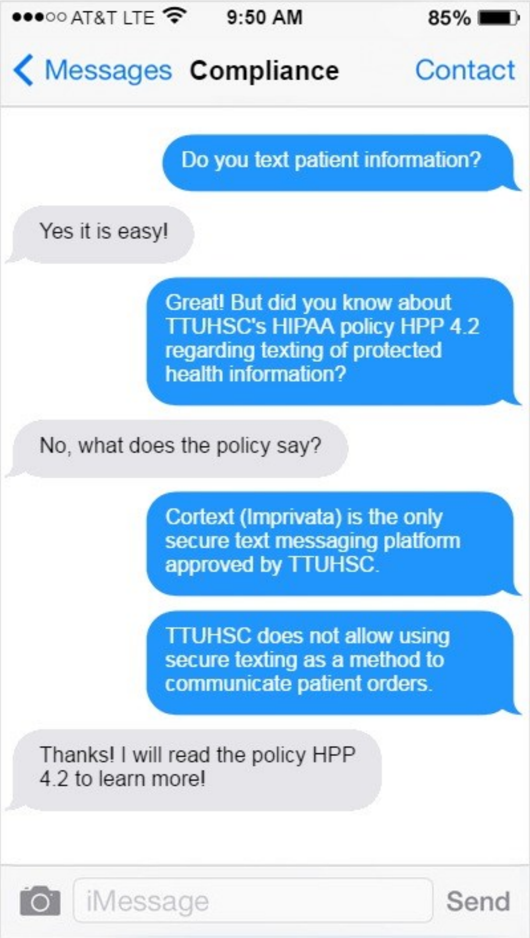
“Tech Support” Scam

This scam involves a criminal posing as a computer support technician that makes an unsolicited call to trick a potential victim into believing his/her computer is infected with malware. A victim is then persuaded to visit websites to download malicious software that gives the criminal the capability to remotely access and control the victim’s machine. Once the criminal has gained the victim’s trust, the criminal charges hundreds of dollars for “phony” assistance with malicious software removal or for the purchase of fraudulent support plans or software. Please remember:

- Hang up the phone if you are suspicious of the caller.
- Never allow a third-party to have remote access to your computer if the caller’s authenticity cannot be verified.
- Do not trust unsolicited phone calls.
- **Never** provide any personal information over the telephone.
- Do not download any unknown software or purchase online services.

If you suspect you are a victim of a tech support scam, immediately change passwords for all accounts including email passwords and online banking accounts; and contact IT Security.

Text Messaging and HIPAA



●●●○○ AT&T LTE 9:50 AM 85%

Messages Compliance Contact

Do you text patient information?

Yes it is easy!

Great! But did you know about TTUHSC's HIPAA policy HPP 4.2 regarding texting of protected health information?

No, what does the policy say?

Cortext (Imprivata) is the only secure text messaging platform approved by TTUHSC.

TTUHSC does not allow using secure texting as a method to communicate patient orders.

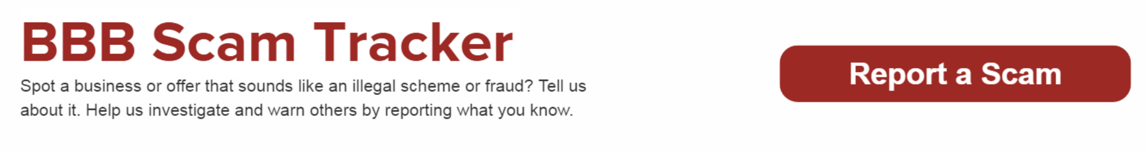
Thanks! I will read the policy HPP 4.2 to learn more!

Protected health information (PHI) is more commonly being communicated and accessed using text messaging. However, HIPAA prohibits the use of text messaging for communicating PHI unless a number of safeguards are implemented.

TTUHSC HIPAA Privacy Policy 4.2 Texting of Protected Health Information defines the accepted practices, responsibilities and procedures for the transmission of PHI via secure text messaging:

- **Cortext (Imprivata)** is the only secure text messaging platform approved for use by TTUHSC health care professionals.
- Cortext is available by contacting the IT Department at each respective campus or calling the Lubbock IT Help Desk at 806-743-1234 .
- All messages that reference a patient should include two patient identifiers in order to confirm patient identity.
- It is HSC's policy **not** to allow secure texting as a method to communicate patient orders.
- Text messages are not stored as part of the medical record.

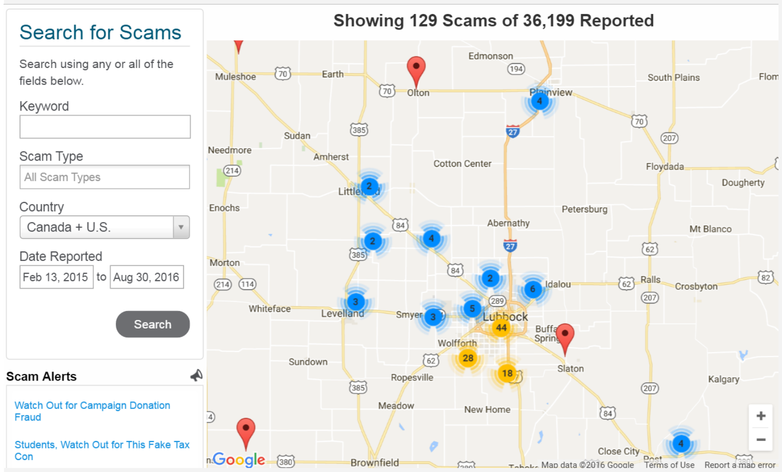
New Tool:



BBB Scam Tracker

Spot a business or offer that sounds like an illegal scheme or fraud? Tell us about it. Help us investigate and warn others by reporting what you know.

Earlier this year, the Better Business Bureau (BBB) launched a website that allows consumers to track scams that have been reported in their area. This is a free platform for information-sharing and awareness of scams in the United States and Canada. The website features a "heat map" that shows the number of scams reported in each area, based on area codes. Also, anyone can use the tracker feature "Report Scam" to provide details such as specific information about the scam; information about the scammer(s); information about the individual(s) scammed; and information about the individual reporting the scam.



Search for Scams

Search using any or all of the fields below.

Keyword:

Scam Type: All Scam Types

Country: Canada + U.S.

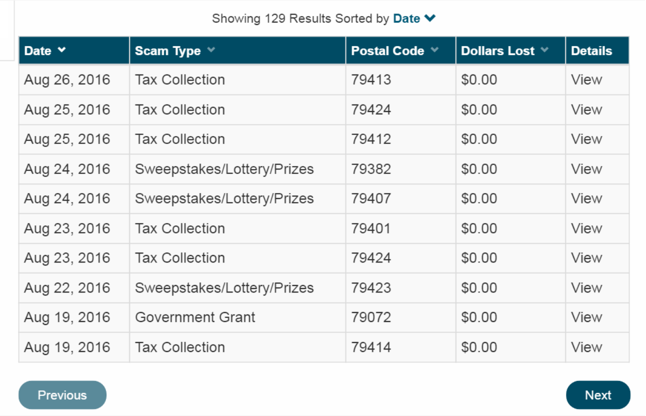
Date Reported: Feb 13, 2015 to Aug 30, 2016

Showing 129 Scams of 36,199 Reported

Scam Alerts

Watch Out for Campaign Donation Fraud

Students, Watch Out for This Fake Tax Con



Showing 129 Results Sorted by Date

Date	Scam Type	Postal Code	Dollars Lost	Details
Aug 26, 2016	Tax Collection	79413	$0.00	View
Aug 25, 2016	Tax Collection	79424	$0.00	View
Aug 25, 2016	Tax Collection	79412	$0.00	View
Aug 24, 2016	Sweepstakes/Lottery/Prizes	79382	$0.00	View
Aug 24, 2016	Sweepstakes/Lottery/Prizes	79407	$0.00	View
Aug 23, 2016	Tax Collection	79401	$0.00	View
Aug 23, 2016	Tax Collection	79424	$0.00	View
Aug 22, 2016	Sweepstakes/Lottery/Prizes	79423	$0.00	View
Aug 19, 2016	Government Grant	79072	$0.00	View
Aug 19, 2016	Tax Collection	79414	$0.00	View

Visit the BBB Scam Tracker website https://www.bbb.org/scamtracker/us for additional information.

HHS

Government Enforcement Update

Advocate Health care Network—$5.55 Million

- On August 4, Advocate Health Care Network (Advocate) agreed to a settlement with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), for multiple potential violations of HIPAA involving ePHI. Advocate has agreed to pay a settlement amount of $5.55 million and adopt a corrective action plan.
- OCR began its investigation in 2013, when Advocate submitted three breach notification reports:

  - On August 23, 2013, Advocate reported that four desktop computers containing the ePHI of approximately 4,029,530 individuals (later amended to 3,994,175) had been stolen from an Advocate Medical Group (AMG) administrative office building, during the early morning hours of July 15, 2013.

  - On September 13, 2013, Advocate reported that, at some point between June 30, 2013 and August 15, 2013, the ePHI of 2,027 AMG patients had been potentially compromised when an unauthorized third party accessed Blackhawk's network. Blackhawk Consulting Group (`Blackhawk") is a business associate of Advocate, which provides billing services to AMG.

  - On November 1, 2013, Advocate reported that an unencrypted laptop containing the ePHI of approximately 2,237 individuals was stolen from an AMG workforce member's vehicle.

University of Mississippi Medical Center—$2.75 Million

- On July 21, the University of Mississippi Medical Center (UMMC) has agreed to settle multiple alleged violations of the HIPAA with OCR. On March 21, 2013, OCR was notified after UMMC's privacy officer discovered that a password-protected laptop was missing from UMMC's Medical Intensive Care Unit (MICU). A directory which contained unsecured ePHI of approximately 10,000 individuals could be easily accessed with a generic username and password.
- During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach, due largely to organizational deficiencies and insufficient institutional oversight. UMMC will pay a resolution amount of $2,750,000 and adopt a corrective action plan to help assure future compliance with HIPAA Privacy, Security, and Breach Notification Rules.

Oregon Health & Science University—$2.7 Million

- On July 18, Oregon Health & Science University (OHSU) has agreed to settle potential violations of HIPAA Privacy and Security Rules following an investigation by OCR that found widespread and diverse problems at OHSU, which will be addressed through a three-year corrective action plan. The settlement includes a monetary payment by OHSU for $2,700,000.
- The investigation began after OHSU submitted multiple breach reports, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive. OCR's investigation further uncovered the OHSU's storage of over 3,000 individuals' ePHI on a cloud-based server without a business associate agreement. OHSU also lacked policies and procedures to prevent, detect, contain, and correct security violations.

TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER™
Office *of* Institutional Compliance

Questions or suggestions? Email shen.wang@ttuhsc.edu
Click here to view past issues of the Compliance Newsletter.

Department Update

Odessa:

The office of Institutional Compliance welcomes a new member to the compliance team:

Tonny Smith is the Permian Basin Billing Compliance Officer starting in August 2016.