○ March ○ 2015

Compliance for you

MARCH NEWSLETTER EDITION

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

Your Compliance Piece

Our Staff Members - In our continuing efforts to strive for excellence, two of our staff have completed new certifications. John Geist has added CHC (Certified in Healthcare Compliance) and Sherri Johnston added CHPC (Certified in Healthcare Privacy Compliance.) Obtaining these certifications involves passing rigorous exams. Congratulations to both John and Sherri.

Annual Billing Compliance Training - It's that time again!
This year, the Billing Compliance Annual Education will focus on Teaching Physician rules, E/M documentation, and some ICD-10 information. The training will be offered online or a department can request a live presentation. To schedule a one hour live training, contact your campus Compliance Office. As always, the online ACME training will include a review test which must be passed with 80% accuracy.

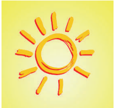
The Drug-Free Schools and Communities Act Amendment of 1989

The Drug-Free Schools and Communities Act Amendment of 1989 requires that students, faculty and staff be informed of the Texas Tech University Health Sciences Center (TTUHSC) program designed to prevent the unlawful possession, use, or distribution of alcohol and illegal drugs. The TTUHSC program includes:

- Standards of conduct prohibiting the unlawful possession, use or distribution of illicit drugs and alcohol;
- Local, state and federal laws and sanctions related to illicit drugs and alcohol;
- The health risks associated with the use of illicit drugs and alcohol;
- Any drug or alcohol counseling, treatment, or other programs available to students and employees; and
- Disciplinary sanctions on students, faculty and staff for violations of drug and alcohol standards of conduct.

Alcohol and Drug Abuse remain a significant problem in the United States and TTUHSC continues to be committed to an environment that discourages the inappropriate or illegal use of alcohol and other drugs.

All TTUHSC students, faculty and staff are encouraged to review the information located at: www.ttuhsc.edu/studentservices or www.ttuhsc.edu/centers/SWIAD/eap/about/faq.aspx#location. Should you have any questions, please do not hesitate to contact the Institutional Compliance Office, Office of Student Affairs, GME Office or the Human Resources Office.



Open Payments Second Year of Data Submission Begins

Physicians and teaching hospitals may now register in the CMS Open Payments system to review any data that may be submitted about them for any payments or transfers of value that occurred in the 2014 calendar year. The review and dispute period for physicians and teaching hospitals is anticipated to start in April 2015.

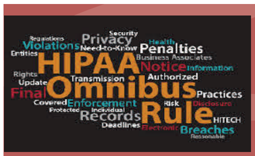
This constitutes the second year of Open Payments data submission, and supports CMS' ongoing efforts to increase transparency and accountability in health care.

- For 2013, CMS reports that the searchable database includes approximately 4.45 million payments.
  - Those payments were made to approximately 545,000 individual physicians and 1360 teaching hospitals, with a total value of nearly $3.7 billion.

As a reminder, payments may include fees for consulting, money for research activities, gifts, speaking fees, meals or travel.

The Office of Institutional Compliance will continue to provide updates about the Sunshine Act Open Payment System. However, we strongly encourage each TTUHSC physician to register with CMS to receive his/her reported payment data. Only physicians and teaching hospitals may review payment information prior to publication.

More information about the Open Payments is available at: www.cms.gov/openpayments. You may sign up for email updates and follow the #openpayments conversation on Twitter.



HIPAA - Myths and Facts

Myth	Fact
Physicians' offices can't use sign-in sheets and can't call out patients' names in the waiting rooms.	False. The HIPAA Privacy Rule does not prevent a health care provider from calling out your name in a waiting room or from a sign in sheet. Sign in sheets can be used, but should only ask for limited information about you, such as your name and appointment time.
Physicians and nurses can't talk about patients where someone might overhear.	False. The HIPAA Privacy Rule does not prevent nurses and doctors from talking about patients in a nurses' station or hallway.
HIPAA doesn't apply to me because I'm not a medical provider or part of a health care institution.	False. The Omnibus Rule now includes enforcement to any business or vendor that "creates, receives, maintains, or transmits PHI". 45 CFR 160 and 164 subparts A and C.
Being HIPAA-compliant is only a compliance concern.	False. It's everyone's concern. Something as small as using a post it note with your username and password on your monitor is a HIPAA violation. Because it can allow someone unauthorized access to PHI.
State laws have no effect on my HIPAA compliant program.	False. Everyone has to consider the HIPAA laws along with their state privacy/security laws, and abide by whichever are stricter.

Anthem Discloses Largest Ever Health Care Industry Cyber Attack

Anthem, Inc., one of the nation's largest health insurers, disclosed on February 4, that hackers had gained access to a database containing the personal information of 80 million current and former members, and Anthem employees. While Anthem reported that credit card numbers and member claims data was not compromised, the hackers did have access to names, Social Security numbers, addresses, dates of birth, employment information and income data.

This is the second large-scale hack on a health care entity to occur recently, after hackers used the "Heartbleed" security flaw to steal approximately 4.5 million patient records from Community Health Systems last year. Shortly thereafter, in April 2014, the F.B.I. issued a Private Industry Notification warning that "the health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely." The F.B.I. Notification cited reports stating that "health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property."

The Anthem news reinforces the warnings from the F.B.I. and highlights the critical importance of strong electronic security measures for all businesses and, in particular, all HIPAA covered entities and business associates.

If you see your passwords on this list, then congratulations - you are using the worst passwords on the Internet.

SplashData has released its annual list of the most common passwords. That popularity also makes them the worst passwords. Here are the top 10.

From Network World | Jan 20, 2015

Rank	Password
1	123456
2	password
3	12345
4	12345678
5	qwerty
6	123456789
7	1234
8	baseball
9	dragon
10	football

CMS to Temporarily Suspend RAC Audits and Make Changes to the RAC Program

On December 30, 2014, the Centers for Medicare & Medicaid Services (CMS) announced that it has evaluated a number of concerns raised about the Recovery Audit Contractor (RAC) Program and is implementing a number of changes. A few changes include:

1. **Look-Back Period.** CMS will now restrict the Recovery Audit Contractor (RAC) program's look-back period to six months from the date of service for patient status reviews.
2. **Audit Timeframes.** Recovery Auditors will now have only 30 days, instead of 60 days, to complete complex reviews and notify providers of their findings.
3. **Discussion Period.** Recovery Auditors must now wait 30 days after their determination before sending the claim's adjustment request to the MAC for recoupment.
4. **Claims Focus.** CMS will require the Recovery Auditors to broaden their review topics to include all claim/provider types, and will be required to review certain topics based on a referral, such as an OIG report. The updated plan also adjusts the level of review based on a provider's denial rates: providers with lower denial rates will have lower levels of review, and rates will be adjusted as a provider's denial rate declines.
5. **Contingency Fee.** Recovery Auditors now will not receive a contingency fee until after the second level of appeal is exhausted.

Guidelines for Chief Complaint

The 1997 Documentation Guidelines for Evaluation & Management Services indicate, "The medical record should clearly reflect the chief complaint." Many providers don't realize that a chief complaint is required for every type of encounter.

It may be a statement from the patient ...

- *"headache"*
- *"shortness of breath"*

It may be a statement from the provider ...

- *"follow-up for hypertension"*

Sometimes the reason may be less specific ...

- *"follow-up of chronic medical problem"*

This is permitted as long as the remainder of the history of the present illness describes the problem that the patient has presented to the provider.

The guidelines also indicate that the chief complaint, review of systems, and the past family social history may be listed as separate elements of history or they may be included in the narrative of the history of the present illness (HPI). As a result, the chief complaint cannot just be anywhere on the record. "It must either be listed separately or in the HPI."

Mobile Device Encryption

Mobile device security presents a number of challenges for many health care organizations. As technology advances, tablets and smartphones become more powerful and useful to the advancement of health care practices. This usefulness also raises several risks for the organization. Mobile devices are easy targets for theft and loss; therefore, data stored on these devices needs to be protected. Encryption is a standard solution and is an effective tool to prevent unauthorized access to any sensitive data. TTUHSC Portable Computing policy can be found at http://www.ttuhsc.edu/it/admin/policy/portable.aspx

Here is how you can set up encryption on your mobile device. For assistance with encryption setup, please contact the IT Solution Center at 743-1234.

Apple iOS (all Apple devices)

- Tap Settings > General > Passcode.
- Follow the prompts to create a passcode.
- After the passcode is set, scroll down to the bottom of the screen and verify that "Data protection is enabled" is visible.

Android 4.4 or lower (most other non-Apple devices)

- Open the Settings menu on your device.
- Under "Personal," touch **Security**.
- Under "Encryption," touch **Encrypt tablet** or **Encrypt phone**
- The "Encrypt tablet" or "Encrypt phone" button will be dimmed if your battery is not charged or your device is not plugged in.
- Touch **Encrypt tablet** or **Encrypt phone**.
- **Warning:** If you interrupt the encryption process before it's completed, you will lose some or all of your data.
- Enter your lock screen PIN, pattern, or password and touch **Continue**.
- Touch **Encrypt tablet** or **Encrypt phone** again.

Android 5.0 or higher (most newer non-Apple devices)

- These devices are automatically encrypted on first use.

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

www.ttuhsc.edu/compliance
806.743.3949

www.ethicspoints.com
1.866.294.9352