TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER™

Compliance Newsletter

September 2017

Texas Tech University Health Sciences Center

Equifax Data Breach: What You Need to Know

According to USA Today, "Credit monitor Equifax announced this month that hackers have gained access to personal information belonging to 143 million U.S. consumers. According to the Federal Trade Commission, if you have a credit report, there's a "good chance" you're one of the 143 million Americans impacted. Here's what you need to know about this most threatening financial data breach in American history.

How could this happen? Equifax failed to promptly install a security fix to a flaw found in a web application tool. Hackers penetrated the company's digital defenses, which allowed them to gain access to the personal data of up to 143 million people. The hackers seized names, Social Security numbers, birth dates, addresses and in some cases driver's license numbers.

How do I know if I was affected? Equifax is still trying to determine how many people were actually affected. Visit Equifaxsecurity2017.com and enter your information to see if Equifax believes your data may have been exposed. The company is also offering free identity-theft insurance, third-party credit-file monitoring, a credit report and other services. You'll have to officially sign up for those services after checking to see if you might be affected.

What are the risks of this hack to me? If you don't take action to protect yourself, hackers could eventually sell your data to other criminals who could then use it to take out loans in your name, get credit cards, perpetuate tax fraud, and access your medical benefits.

How can you protect yourself? Experts say freezing your credit is one line of defense. That way, if criminals try to use your personal data to take out a loan, credit or services in your name, they will probably get turned down because your credit report cannot be pulled. Other important steps: monitor your bank records, credit card charges and other bills carefully — ideally once a week.

How do I freeze my credit?

To place a freeze on your credit reports, you need to call the credit reporting companies: Equifax, Experian, TransUnion, and Innovis. It is recommended to freeze your credit at all four. Fees vary by state and range from about $5 to $10. Equifax has temporarily waived its fees for this service."

Read the full article here: Equifax data breach: What you need to know about hacking crisis

TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER™

Compliance Newsletter

September 2017

Yes, Staff Snooping of Medical Records is a Privacy Breach

According to Medical Economics, "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 incident may seem harmless, they still constitute privacy breaches, and carry all the same risks." Read the full article here: Yes, staff snooping of medical records is a privacy breach

"UCLA Medical Center fired at least 13 employees and suspended at least six others for snooping in the medical records of pop star Britney Spears during her hospitalization in its psychiatric unit in 2008. In addition, six physicians faced discipline."
- Los Angeles Times

United Healthcare Commercial Reimbursement Policies
Revision to the Consultation Services Reimbursement Policy

Effective for claims with dates on or after Oct. 1, 2017, United Healthcare will reimburse the appropriate evaluation and management (E/M) code which describes the office visits, hospital care, nursing facility care, home service or domiciliary/rest home care reported in lieu of a consultation services procedure code.

United Healthcare will align with the Centers for Medicare & Medicaid Services (CMS) and no longer reimburse consultation services represented by CPT codes 99241-99245 and 99251-99255. At the time of the original CMS decision to no longer recognize these consultations services procedure codes, United Healthcare began pursuit of data analysis and trending to better understand the use of consultation services codes as reported in the treatment of their commercial member. According to their data analysis, misuse of consultation services codes was revealed.

The current Relative Value Unit (RVU) assignments reflect numerous changes made during recent years to both E/M codes and other surgical services creating an overall budget neutral experience supporting this strategy as a more accurate reflection of services rendered.

Compliance Newsletter

September 2017

Texas Tech University Health Sciences Center

E/M coding

Know Scenario 4 Documentation Guidance

In Transmittal 2303, CMS adds "Scenario 4" to the list of common scenarios for teaching physicians providing evaluation and management (E/M) services:

"**When a medical resident admits a patient to a hospital late at night and the teaching physician does not see the patient until later, including the next calendar day:**

- The teaching physician must document that he/she personally saw the patient and participated in the management of the patient. The teaching physician may reference the resident's note in lieu of re-documenting the history of present illness, exam, medical decision-making, review of systems and/or past family/social history provided that the patient's condition has not changed, and the teaching physician agrees with the resident's note.

- The teaching physician's note must reflect changes in the patient's condition and clinical course that require that the resident's note be amended with further information to address the patient's condition and course at the time the patient is seen personally by the teaching physician.

- The teaching physician's documentation **must reflect the date of service he/she saw the patient** and his/her personal work of obtaining a history, performing a physical, and participating in medical decision-making regardless of whether the combination of the teaching physician's and resident's documentation satisfies criteria for a higher level of service. For payment, the composite of the teaching physician's entry and the resident's entry together must support the medical necessity of the billed service and the level of the service billed by the teaching physician."

CMS describes minimally acceptable documentation for this scenario as being:

* Initial Visit: "I saw and evaluated the patient on _____(date). I reviewed the resident's note and agree, except for …….

* Initial or Follow-up Visit: "I saw and evaluated the patient on _____(date). Discussed with resident and agree with resident's findings and plan as documented in the resident's note."

Examples of unacceptable documentation for this scenario:

* "Agree with above," followed by legible countersignature or identity

* "Rounded, Reviewed, Agree," followed by legible countersignature or identity

* "Discussed with resident. Agree," followed by legible countersignature or identity

Such documentation is not acceptable because it does not make it possible to determine whether the teaching physician was present, evaluated the patient, and had any involvement with the plan of care.

Read the complete Transmittal 2303 here:
Transmittal 2303

**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.