JUNE | 2016

Compliance *for you*

Health Care Vendor Access & Vendormate

Did you know that Vendors are required to sign in when they visit TTUHSC? Have you heard of Vendormate? Below are some of the most frequently asked questions regarding Vendor access & Vendormate:

1. Who is considered a Health Care Vendor?

Health Care Vendor is any individual or company that sells or markets health care services or items to TTUHSC and/or its patients, including, but not limited to pharmaceutical companies and their representatives, device or durable medical equipment (DME) manufacturers and their representatives, and equipment and/or service providers, and their representatives.

2. How does TTUHSC manage Health Care Vendor access?

TTUHSC has contracted with Vendormate, a vendor credentialing company, to provide education, maintain an online repository of required vendor data, and provide a tool to print real time badges for proper vendor registration. For more information, please refer to TTUHSC policy HSC OP 52.16 Health Care Vendor Interactions.

3. How does Vendormate work?

Any Health Care Vendor seeking access to TTUHSC facilities, clinics, faculty or residents shall register with Vendormate before their representatives are allowed onto a TTUHSC campus, site, or facility. Health Care Vendors are required to check-in and receive an ID badge each time they enter a TTUHSC facility, clinic, office and/or department. The Vendormate Check-in station at Lubbock is located at the front desk of the Texas Tech Physicians Medical Pavilion.

4. What is expected from TTUHSC employees?

Employees should require vendors and reps to register through Vendormate before agreeing to meet with them or allowing them onto TTUHSC premises.

Remember, reps should always wear Vendormate ID badges.

If you see a rep walking in your clinic without ID badge, you should ask him/her if they have checked in at the front desk. If not, you should ask the rep to register using Vendormate.

For more information, please visit COIC webpage. *More Q&As are coming!*

2016 Conflict of Interest and Commitment (COIC) Training & Disclosure

In May 2016, the Office of Institutional Compliance deployed the new Conflict of Interest and Commitment Training & Disclosure Module. Starting this year, all employees of TTUHSC are required to complete COIC training which will be followed by a disclosure form. If you have not done so, click here to complete the Training & Disclosure. You have until August 1, 2016 to meet this requirement!

Critical Care E/M Coding

Are your critical-care claims at risk for denial or repayment upon review?

Critical Care is the direct delivery by a physician of medical care for a critically ill or critically injured patient. Critical illness acutely impairs one or more vital organ systems such that there is high probability of imminent or life threatening deterioration in the patient's condition. Below are some tips for critical care E/M coding:

- The CPT codes for Critical Care are 99291 (30-74 minutes) and 99292 (each additional 30 minutes). Less than 30 minutes should report appropriate E/M codes.
- Time spent on critical care does not need to be continuous. The time spent on critical care does not need to be spent in face-to-face care of the patient, but must be spent in the location where the critical care is being performed. The total time billed for critical care must be recorded in the chart.
- Critical care does not need to be provided solely in an intensive care unit.
- A split/shared E/M service performed by a physician AND qualified NPP of the same group practice (or employed by the same employer) cannot be reported as critical care service. Service cannot be combined.
- Teaching Physicians must be present for the period of time for which the claim is made. Only time spent by the resident and TP together with the patient or the TP alone with the patient can be counted. Time spent by the resident in the absence of the TP is not billed.
- The following services are included in critical care and should not be reported separately.

1) Cardiac output measurements
2) Chest x-rays interpretation
3) Pulse oximetry
4) ABGs
5) EKG interpretation
6) Gastric intubation
7) Transcutaneous pacing
8) Ventilator management
9) Peripheral venous access
10) Arterial puncture

Read More Here in Section 30.6.12

The Dangers of Copy and Paste

In electronic health records systems (EHRs), the Copy and Paste function provides the ability to reuse parts or all of the detailed information, which is a great time saving tool for Physicians and EHRs users. Copying and pasting of healthcare documentation from previous medical record entries has become a common practice. According to a study published in 2009, 90 percent of physicians use the Copy and Paste functionality in daily progress notes.

However, using the Copy and Paste function without careful review can lead to serious consequences. In 2014, the American Health Information Management Association (AHIMA) published a position statement to address the use of Copy and Paste functionality in EHRs. AHIMA has also identified a number of challenges and risks associated with Copy and Paste function:

- Inaccurate or outdated information
- Redundant information, which makes it difficult to identify the current information
- Inability to identify the author or intent of documentation
- Inability to identify when the documentation was first created
- Propagation of false information
- Internally inconsistent progress notes
- Unnecessarily lengthy progress notes

Although the Copy and Paste feature can enhance efficiency of data entry, it may also facilitate attempts to inflate, duplicate, or create fraudulent health care claims. When you copy and paste a note, make sure each note reflects the documentation needs of a specific encounter.

Read More: 5 Ways to Avoid Copy and Paste Errors

TTUHSC Safe Computing Tips

►Use of Removable Media (USB Storage, External Hard Drives, Backup Solutions)

Storing of sensitive/confidential data on removable media is discouraged. If there is no other alternative the removable media must be encrypted using TTUHSC encryption technologies.

Instructions on how to encrypt removable media can be found at SolveIT Website.

►Portable Computing Devices (Laptops and Tablets)

Storing of sensitive/confidential data on portable computing devices is discouraged. It is understandable that the storing of sensitive/confidential data is unavoidable, which would require the portable computing device to be encrypted. TTUHSC IT can encrypt both laptops and tablets that are institutionally owned. Encryption of laptops and tablets protect the sensitive/confidential data from unauthorized access should the device(s) be lost or stolen.

TTUHSC policy regarding encryption is at:

Institutional IT Policy Site

To schedule an appointment to have your device encrypted contact the IT Solution Center at:

www.ttuhsc.edu/it/stars

►Email - Phishing Attacks and Spear Phishing Attacks

TTUHSC will never ask you to provide your password via phone or email. Your password is something that you and you alone should know. Attackers are constantly trying to trick users into providing their eRaider user name and password. Once an attacker has your eRaider user name and password the attacker can do all of the following:

- Access all of your email (read it, delete it, send email as you).
- Change your TTUHSC direct deposit information (get your paycheck).
- Search your email for sensitive information.
- Use your email to try and obtain more TTUHSC users to provide their user name and password.
- Use your email address to send malicious email.

If you think your user name and password have been compromised you should do the following:

- Change your password immediately at here
- Contact the IT Solution Center at: 806.743.1234
- Provide any suspicious emails as an attachment to: itsolutions@ttuhsc.edu
- Verify your banking information has not changed at: https://webraider.ttuhsc.edu
- Common questions regarding passwords can be found here.

►Email - Sending Encrypted Email

As a part of normal business, users at TTUHSC will need to send sensitive/confidential information to business partners, sister hospitals, etc... To accomplish this TTUHSC has implemented email encryption appliances to allow for the sending of sensitive information encrypted to maintain compliance with state and federal regulation. However, TTUHSC does not allow sensitive/confidential information to be sent to public email domains (Gmail, Yahoo, AOL, etc.) unless specifically requested by a patient through the TTUHSC Medical Records Department.

- To send an encrypted email you need to type [ss] or [send secure] in the Subject Line of the email you wish to send encrypted.
- If an email you sent is flagged for automatic encryption, you will receive a notification that your message was encrypted.
- Information regarding email encryption can be found at: SolveIT Website.
- Policy information regarding email encryption can be found here.

►Security Awareness- Be Ready for Whatever Comes Your Way

In today's digital world it is not always easy to know what is malicious or not. Security awareness training provides the TTUHSC user base with the knowledge to detect, avoid, and report security related issues as they encounter them. TTUHSC utilizes digital signage, email announcements, and a fully interactive training program to educate users on security issues.

Security awareness training

Policy regarding security awareness training

Know or Suspect a Breach Incident? What Should I Do?

If a TTUHSC workforce member knows of or suspects a breach of protected health information (PHI) or personal information, it is the employee's responsibility to report actual or suspected violations of confidentiality to the TTUHSC Regional Privacy Officer or the department supervisor, or they can report it anonymously through the Compliance Hotline located on the TTUHSC website or by calling 866-294-9352. Failure to report a known HIPAA violation may result in disciplinary action in accordance with TTUHSC policies. Workforce members should be knowledgeable of the types of HIPAA violations that could be considered a breach of PHI. Examples of reportable HIPAA violations include, but are not limited to the following:

- Mistakenly sending e-mails or faxes containing PHI to the wrong recipient.
- Discussing PHI in public areas where it can be overheard, such as elevators, cafeteria, restaurants, hallways, etc.
- Leaving PHI in a public area.
- Leaving a computer accessible and unattended with unsecured PHI.
- Loss of an unencrypted electronic device containing unsecured PHI.
- An individual fails to report that his/her password has been potentially compromised (i.e., has responded to e-mail spam giving out his/her password).
- Intentional, unauthorized access to friends, relatives, co-workers, public personality's or other individual's PHI.
- Intentionally assisting another individual to gain unauthorized access to PHI. This includes, but is not limited to, giving another individual your unique user name and password to access electronic PHI.
- Failing to properly verify the identity of individuals requesting PHI which results in inappropriate disclosure, access or use of PHI.
- Connecting devices to the network and/or uploading software without having received authority from IT.

Please contact your campus' Regional Privacy Officer or

the Office of Institutional Compliance if not sure whether an issue is a breach.

We are happy to assist as we all work together to protect our patients' information.

"How many compliance officers does it take to change a light bulb?"
"Three. One to change it, one to check it and one to check it again and file a report."

"Why did the compliance officer laugh three times at the joke? "
"Once when it was told, once when it was explained and once when they understood it ."

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 Updates

Lubbock:

Corlis Norman, Billing Compliance Director, has retired on May 31, 2016.

Amarillo:

As of May 31, 2016, Alicia Copeland, Amarillo Privacy Officer, is no longer with TTUHSC.