EVMS MEDICAL GROUP

Compliance Newsletter

July 2018 Volume 20, Number 7

In This Issue

- **Physical Security**
- **Responding to Audits: Facilities**
- **e-PHI Security Tip**
- **Lunch Discussion August: Patient Registration**

Compliance Hotline

Type:

http://157.21.29.163/Compliance/

and click on Hotline.

EVMS Medical Group Compliance concerns may also be sent to the EVMS Medical Group Compliance Office via phone, mail or e-mail.

Physical Privacy & Security in the Office

It is very important to periodically assess physical security in your office space. The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) publishes a monthly newsletter on different cybersecurity issues and the May edition focused on physical and workstation security. The newsletter provides prompts or questions to think about when formulating a physical security strategy to include the following:

- Is there a current inventory of all electronic devices such as computers, portable devices, or other electronic media in the office and where are these items kept?
- Are any devices in public areas or other places that make them more vulnerable to theft, unauthorized use, or viewing?
- Should devices currently in public or vulnerable areas be relocated?
- What physical security controls are currently in use (i.e., cable locks, privacy screens, secured rooms, cameras, guards, alarm systems) and are they easy to use?
- What additional physical security controls could be reasonably put into place?
- Are policies in place and employees properly trained regarding physical security (i.e., use of cable locks and privacy screens)?
- Are signs posted reminding personnel and visitors about physical security policies or monitoring?

The OCR also notes that "Investigations by the U.S. Dept. of Health and Human Services Office for Civil Rights (OCR) that have included, among others, potential violations of the Security Rule's Workstation Security standard have resulted in settlement payments by covered entities ranging from $250,000 to $3.9 million." This is an issue that is taken very seriously by our enforcement agencies and therefore it is important for us to monitor. If you would like to schedule a time for the Compliance Office to conduct a physical security audit, please feel free to do so. For more information, please visit the May 2018 HHS Cybersecurity

Contact Us

EVMS Medical Group Compliance Office
4111 Monarch Way,
Suite 500
Norfolk, VA 23508
Phone 451-6200

Link to Policies & Forms:
http://www.evms.edu/patient_care/compliance_program/

James F. Lind, Jr., MBA
Compliance Officer

Privacy Office
Privacy Line 451-6298

Leanne Smith, CHC
Administrator

Laura Brower, CHC, CPC
Coding & Compliance Manager

Donita Lamarand, RN, BSN, CPHRM
Director of Risk Management

Andrea Willis, CPC, CPMA
Clinical Auditor

Compliance "Listserv"

Send an email to browerl@evms.edu to request to be added to the EVMS Medical Group Compliance "Listserv". Once you are subscribed, you will receive newsletters, information and training opportunity announcements directly.

Newsletter at the link below:

HHS Cybersecurity Newsletter May 2018: Workstation Security

Responding to Audits: External Facilities

Many of our providers see patients at hospital, nursing, and other facilities in addition to our office facilities. Typically documentation for those services is created and stored in the system used by that facility to which the provider has been given access. Although we do not maintain that documentation within our Electronic Health Record (EHR), we are responsible for any and all documentation that supports the services will bill.

For all audits, both conducted by our internal audit program and those performed by external entities such as insurance carriers, we must gather any documentation maintained outside of our EHR and provide it to the auditing entity to support services billed. For outside audits this must usually be done within 15-45 days depending on the request. When an internal audit is performed, the auditor will send the invoices to management at the department and request that documentation be returned for review. This information should be obtained within 30 days at the most.

If information from external facilities is not received for either external and internal audits, payment for that service will be retracted or returned to the payer. It is important that each department and division have a process for obtaining this information in a timely manner. If there are issues with access that are due to the facility itself, those issues should be addressed at the contact level with the facility. If your department has questions or concerns about obtaining documentation for services billed from an external facility please feel free to reach out to the Compliance Office for additional information or advice on how to proceed.

e-PHI Security Tip

Social engineering is a type of attack in which the attacker uses information about the organization to target specific individuals or gain unauthorized information. Social engineering could be conducted over the phone, by email, or in person. This person may ask for login credentials, information about employees, or impersonate others. To protect against social engineering, remember that you should never give someone access to your password by phone and that it is not typical for internal employees to call asking for personal or sensitive information. Anything out of the ordinary should be questioned or double-checked!

Lunch Discussion Session August

Topic: Patient Registration

Who Should Attend: All staff members who are responsible for registering new patients as well as managers and supervisors. It is very important for managers to understand and be able to convey this information to new staff and existing staff who need retraining.

Date and Location:
Thursday, August 16th, 12-1:00 pm in HH 758

Please RSVP to Leanne Smith at smithlf@evms.edu or 451-6207 and feel free to bring your lunch!