EVMS
MEDICAL GROUP

Compliance Newsletter

June 2018 Volume 20, Number 6

In This Issue

Duplicate Medical Records

The number of duplicate patient medical records has been steadily increasing. Duplicate medical records are created when a thorough search for the patient is not completed upon registration. Duplicate records are an issue for the following reasons:

- Patient safety. Patients with multiple records may have treatment information, labs, medications, and other important health information in different charts. This could lead to inappropriate care due to lack of accurate information.
- Billing/claims processing. If the patient's information is incorrect or incomplete the billing and claims process will be inefficient or unable to proceed.
- Administrative organization/efficiency. Looking up a patient who has multiple records is cumbersome and can be confusing. Once a duplicate record is created the next individual to look that patient up may need to do extensive research to locate the correct patient and those records will need to be merged.

To avoid creating a duplicate medical record, staff should begin by looking up the patient by searching for the first three letters in the last name followed by the first three letters of the first name in IDX. Once a list is displayed, the date of birth and other identifiers can be matched. Other strategies include using an exact match to the patient's legal identification, verbally asking them to spell their full legal name, and asking if they have previously used another name or were recently married. It is also worth noting that we cannot require a patient to provide a Social Security number so that identifier should not be solely relied upon. Although pre-printed registration forms may be used, staff should also be verbally verifying important demographics with patients each time an update is necessary. Training materials for registration issues are available upon request.

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.

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.

Access Termination Procedures

If not already maintained, management in each department should have a database that lists all systems containing PHI and what individuals within the department have access to them. This list could include Allscripts, IDX, EPIC (Sentara or Bon Secours), and any other systems used in the office to include eligibility systems, office equipment, etc. When granting access, a unique profile should be set up for each staff member based on his or her needs and job function. Mirroring is discouraged as staff members may have different tasks even if their title or role is the same.

When an employee leaves the practice, having a list as described above makes it much easier to remember the systems from which that individual needs to be terminated. This should include any temporary employees or individuals with access for other purposes such as research which are harder to identify since they are not included in the daily termination list from Human Resources. This process also makes it easier to provide notification to any outside entities such as Sentara and/or Bon Secours. It is important to remember that we are responsible for our employee's access to those systems as well.

e-PHI Security Tip

Password requirements can seem excessive and the many different passwords needed for multiple systems can sometimes make them difficult to remember. If you need to use a system to track passwords, best practice is to do so **on paper** and lock in a secure, private, location. It is also best to use prompts or reminders rather than to write out the full password. Never store passwords in any digital format to include a Word Document or in Outlook. If a hacker gains access to your desktop or email they will then be able to access all systems with a list of your passwords!

Lunch Discussion Session July

Lunch Discussion is cancelled for the month of July.