EVMS
MEDICAL GROUP

Compliance Newsletter

September 2013

Volume 15, Number 9

In This Issue

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.

CMS Open Payments Program Updates

The June 2013 EVMS Medical Group Compliance Newsletter described the CMS Open Payments Program for transparency in detail. This program is important because collaboration among physicians, teaching hospitals, and industry manufacturers can contribute to the design and delivery of life-saving drugs and devices, however, while some collaboration is beneficial, payments from manufacturers to physicians and teaching hospitals can also introduce conflicts of interests. Knowledge of these financial relationships is also important because it encourages a closer examination of their intent as well as the possible unintended negative effects on patient care and treatment choices.

Additional information is being regularly released on this program and CMS has recently provided new resources for education and tracking:

- Two Continuing Medical Education activities have been released as additional resources:
    1. “Are You Ready for the National Physician Payment Transparency Program?”, which provides general information on the Open Payments Program
    2. “The Physician Payment Transparency Program and Your Practice”, which details transfers of value, types of transfers, and how to track payments.
- A mobile app has been developed for physicians called Open Payments Mobile for Physicians. The app is for personal information collection and storing of payments throughout the year to help with tracking.

As a reminder, the initial reporting period began on August 1, 2013 and runs through December 31, 2013. Collected data for this period must be submitted to CMS (by the industry) by March 31, 2014. Providers and hospitals will have 45 days to review and request corrections to information submitted about them. Reported data will be publically available by September 30, 2014.

Contact Us

EVMS Medical Group Compliance Office

4111 Monarch Way,
Suite 500
Norfolk, VA 23508
Phone 451-6200

www.evmsMedicalGroup.com

James F. Lind, Jr., MBA
Compliance Officer

Privacy Office
Privacy Line 451-6298

Leanne Smith, CHC
Administrator

Pamela Wheeley, CPC
Compliance & Internal Audit Specialist

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

Laura Brower
Administrative Coordinator

More information is available by sending questions to openpayments@cms.hhs.gov or visiting the website at:

http://go.cms.gov/openpayments

HIPAA Audits

Various aspects of healthcare reform have brought with them the increased potential and possibility for an array of different types of audits. The American Recovery and Reinvestment Act of 2009, which requires periodic audits to ensure that covered entities are HIPAA compliant, has made the chance of being audited for compliance and privacy increasingly possible, and it is still becoming more likely. A pilot program conducted by the Office of Civil Rights (OCR) in 2011 audited 115 covered entities and audits have since expanded and become mandatory under HITECH. Significant dollars have already been recovered in settlements for discovered HIPAA violations.

The audit structure centers around three elements:

- Privacy: policies and procedures, access to and uses and disclosures of PHI
- Security: physical, technical and administrative safeguards
- Breach Notification: policies and procedures and corrective actions

Based on the pilot program the Office of the Inspector General (OIG) identified 124 high impact vulnerabilities that covered entities should self-audit to prepare for these audits and ensure their compliance. A few items from these recommendations include:

- Are your policies and procedures updated and compliant, accessible by staff, and are changes regularly published for staff awareness?
- Is there a written compliance plan or risk assessment plan and are staff aware of it? Are all compliance problems reported and tracked?
- Are there employee training materials and do staff participate in training? How often is it maintained and are logs kept?
- What policies are there for mobile devices and what encryption technology is present? Stolen laptops, tablet computers, and smart phones account for many security breaches and internal controls should be implemented.

These are a few examples of things we should be thinking about not only in the event of an audit, but to prevent breaches in the first place. Staff buy-in to compliance and privacy policies and adherence is extremely important to patient protection and safety.

Compliance Discussion Group for October 2013

Topic: Annual Compliance Training

Dates and Locations:
Tuesday, October 15, Hofheimer Hall 752
Thursday, October 17, Hofheimer Hall 752

Time:
Noon to 1:00.

RSVP by email or phone to Laura Brower (451-6202) or Leanne Smith (451-6207).

Bring your lunch