March 30, 2010

"TIPS" Newsletter
HIPAA Privacy Series FAQ's 3rd in Series

By Edie Hofmann (Edie Ruark Dahlhauser), President ICCOM, LLC
edie@ICCOM.org

You need to know about HIPAA Privacy and Security. This is the third in a series of FAQ's about HIPAA Privacy and Security to help you understand your responsibilities under the HIPAA Rules. Are you HIPAA compliant?

The full HIPAA Privacy and HIPAA Security Compliance Checklists are available on our website:
HIPAA Privacy Checklist
HIPAA Security Checklist

HIPAA Privacy and Security, FAQ's .....Continued

Patient Compliants

Are we required to have a formal privacy complaint process related to privacy issues?

HIPAA mandates a process for individuals to complain to both the practice and the Secretary of Health and Human Services (HSS) about either the practice's policies and procedures related to privacy or compliance with the policies and procedures or the requirements.

Are there specific requirements about notification?

The final Rules stipulate that covered entities have a mechanism for receiving complaints and this mechanism must be included in the Privacy Notice (specify contact person or office phone number).

Do I have to keep a record of complaints?

Yes, you have to maintain a record of the complaints you receive and a brief description of the resolution, if there is a resolution.

Can the individual elect to complain to the Secretary of Health and Human Services (HSS) without first complaining to me, as the practice?

Individuals have the right to send their complaint directly to the Secretary of HSS.

Are there specific requirements for filing a complaint with the Secretary of Health and Human Services (HSS)?

Complaints must be in writing (either on paper or electronic), must name the practice, and must be filed within 180 days of when the complainant knew or should have known of the omission.

What could happen if the Secretary of Health and Human Services (HSS) found the complaint to substantiate a violation?

Efforts would be made to settle the matter informally with the practice. A compliance review of the practice might result. If the Secretary of HSS found no violation, the practice and the complainant would be notified. A practice that is found to have violated the Privacy Regulations may face civil penalties up to $100 per violation and/or criminal penalties if the practice knowingly violated the Privacy Regulations. Criminal penalties can include substantial fines as well as incarceration.

Privacy Official

What is the intent or purpose of the privacy official?

The privacy official is responsible for implementing and overseeing the privacy policies and procedures for the practice. He/she oversees all activities related to the development, implementation, maintenance of and adherence to the practice's policies and procedures addressing privacy and access to protected health information (PHI). He/she assures compliance with HIPAA and all other federal and state rules and regulations pertaining to use and release of PHI.

Small practices may assign this role to one or more persons, while larger group practices most likely will designate a specific person to oversee the integrity of PHI. The privacy official has numerous roles such as performing a risk assessment of the practice to determine where vulnerabilities lie with respect to PHI and ensuring that privacy security measures and policies are implemented and adhered to by the practice. He or she serves as the designated contact person required by the final Rule to receive complaints and provide further information about the practice's privacy policy procedures.

What steps or activities should be privacy official take to assure compliance?

Key activities are really basic risk management techniques. A privacy official should conduct the following steps:

A. Identify the internal and external risks of disclosure of protected health information (PHI).

B. Create a plan to reduce the risk of releasing PHI in those areas identified.

C. Implement the plans.

D. Train all personnel on the practice's privacy and security of PHI.

E. Monitor the implementation and enforce appropriately any breaches of policy.

Identifying the risks of disclosure is the first step so policies and procedures can be created to address the use and release of PHI. A risk assessment should be conducted to ascertain where privacy and security threats may exist. Make a list of all activities that involve the use or disclosure of PHI and evaluate whether there are policies and procedures already in place to reduce the risk of release.

Once areas are identified, create a plan of action around those areas identified to reduce the risks. The plan development communicates to staff the importance to the practice of the safe and proper utilization of protected health information.

Policies and procedures should be modified or developed to integrate compliance into everyday activities. Implementation of the plan should consider the needs and ability of the staff to assimilate and follow the policies and procedures. It applies to the actual health care records as well as electronic or computerized records containing PHI.

During implementation, all personnel must be trained in the relevant areas that affect their interaction with PHI. Staff must understand what information is protected, when PHI may be released, and when PHI may be in jeopardy of improper release. Training should be integrated into the practice's compliance plan including documentation of the training that has occurred. The training is germane to the responsibilities of the staff member. Changes in job descriptions or positions that allow greater access warrants additional training within a reasonable time frame following the change in responsibilities.

Monitoring is an important part of the privacy official's duties. This means actively checking to make sure the practice is adhering to the policies and procedures related to PHI. It is important to always follow your own rules to mitigate the opportunity for an error to occur but also reduce the damage if improper use or release is detected.

What if information is misused or improperly released?

HIPAA requires that health care practices provide a complaint process to individuals who feel the practice is not following their own policies and procedures. **As privacy official, you** need to implement this process if it is not in place already. This complaint process allows

individuals to resolve complaints at both a local and a federal level.

What qualifications and responsibilities should a privacy official's job description contain?

The Microsoft Word document within this manual is a sample privacy official job description developed by the American Health Information Management Association (AHIMA).

(to be continued)

==========

Please visit my website that further explains the HIPAA rules and more about the compliance manuals available.

http://www.iccom.org/index_files/ICCOMProducts.html

email me with any questions you may have: edie@iccom.org