May 9, 2014

HIPAA Back-to-Basics Bulletin Series
Roles and Key Functions of Privacy and Security Officers

This is the third in a series of bulletins going "Back to Basics" on HIPAA compliance. With the recent changes to HIPAA resulting from the Omnibus Final Rule, this is a good time to reevaluate your organization's compliance with all aspects of HIPAA.

Under the HIPAA Privacy Rule every covered entity is required to designate a privacy officer; conversely, the HIPAA Security Rule requires designation of a security officer. Although these officers may have other titles and duties within your organization, they must be fully committed to the privacy and security compliance for which they are tasked.

Your organization should determine the qualifications necessary for each position. For example, we suggest that the holder of each position meet the following criteria:

- Trained in or knowledgeable about privacy or security regulations (as applicable), health care facility operations and electronic information flow and dissemination;
- Possesses substantial decision-making authority and discretion with respect to the operations of your organization, including sufficient authority to take or direct steps that may be necessary to maintain compliance (e.g., authorizing expenditures, assigning personnel, etc.);
- Willing and able to devote the time necessary to ensure effective implementation and operation of a privacy and security compliance program;
- Has not been found to be in violation of any laws or policies of your organization; and
- Possesses values and principles that are representative of your organization.

The privacy officer is charged with developing and implementing the organization's privacy policies and procedures and for assuring compliance with federal law, and must be committed to patients' privacy and confidentiality. Some of the key functions of the privacy officer include:

- Designing, implementing and operating the privacy compliance program;
- Monitoring the effectiveness of the privacy program on a regular basis, including a comprehensive review conducted at least annually; and
- Enforcing the standards and fully investigating possible violations, including imposing or recommending sanctions for violations of standards.

Similarly, the security officer is charged with developing and implementing security policies and procedures and for ensuring compliance with policies and federal law and must be committed to electronic information security. At a minimum, the security officer should:

- Draft and revise necessary policies and procedures for the organization;

- Conduct a security risk assessment, at least annually, and develop policies and protocols for mitigating any security violations; and
- Develop policies and protocols for protecting electronic patient information against security and privacy violations.

INCompliance offers customized HIPAA consulting services, including assisting your organization with selecting and training privacy and security officers, and policy and procedure development. Click here for additional information on our services.

This E-Alert was prepared by Bryn Hunt. Bryn can be reached 614.227.4823 or bhunt@incomplianceconsulting.com. Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com. This E-Alert may be accessed on the INCompliance website.