LEGAL COUNSEL BENEFITING YOU
HAYNES BENEFITS PC

HIPAA SECURITY, PORTABLE ELECTRONIC DEVICES AND OFFSITE ACCESS: ARE YOU SECURE?

The HIPAA Security Rule requires all covered entities to review and, where needed, modify security policies and procedures on a regular basis.[1] The Department of Health and Human Services (HHS) recently issued guidance that covered entities may rely upon to determine if their actions are reasonable and appropriate for safeguarding Electronic Protected Health Information (e-PHI).

Due to their heightened vulnerability, HHS is concerned with the following kinds of devices and tools: laptops; home-based personal computers; PDAs and Smart Phones; hotel, library or other public workstations and Wireless Access Points; USB Flash Drives and memory cards; floppy disks; CDs; DVDs; backup media; email; smart cards; and Remote Access Devices.

HHS provides the general warning that covered entities should be extremely cautious about allowing the offsite use of, or access to, e-PHI. Specifically, offsite access is only appropriate "when it is clearly determined necessary…, and then only where great rigor has been taken to ensure that policies, procedures and workforce training have been effectively deployed, and access is provided consistent with the applicable requirements of the HIPAA Privacy Rule."[2]

The HHS guidance calls specific attention and emphasis to the following three areas:

1. Risk analysis and risk management strategies;
2. Policies and procedures for safeguarding e-PHI; and
3. Security awareness and training on the policies and procedures for safeguarding e-PHI.

Risk Analysis and Risk Management Strategies. HHS groups the risks associated with remote access and offsite use of e-PHI into three areas:

1. Access. Focus on ensuring that users only access data for which they are appropriately authorized.
2. Storage. Address the security requirements for media and devices which contain e-PHI and are moved beyond the covered entity's physical control.
3. Transmission. Ensure the integrity and safety of e-PHI sent over networks.

[1] 68 FR 8334.
[2] 67 FR 53182.

The guidance provided by HHS includes a table listing risks associated with each above category paired with appropriate risk management strategies. The strategies for each risk range from basic to complex. This table is an extremely helpful tool in light of the statement by HHS that covered entities may rely upon this guidance. Thus, the guidance provides somewhat of a safe harbor.

Policies and Procedures for Safeguarding e-PHI. A thorough risk analysis and review of possible risk management strategies will lead to the establishment of suitable policies and procedures. Covered entities must appropriately document these policies and procedures.

For more information, please contact Haynes Benefits at 816.875.1919 or visit
www.haynesbenefits.com