Health Information Compliance Alert

Reader Question: Do You Need To Comply With PCI Standards?

Question: Our practice accepts credit and debit card payments from patients. Does this mean we need to comply with the Payment Card Industry (PCI) security standards, even if we're already in compliance with HIPAA Security Rule standards?

Answer: You know that you have to comply with HIPAA, but you need to comply with PCI standards too. Retailers and financial institutions have been undertaking efforts for quite some time to address PCI standards to ensure the security of their transactions and the protection of customers' credit/debit card information, according to an Oct. 28 blog posting by **Mark Burnette, CPA, CISSP, CISM**, a partner with **LBMC Information Security**.

"But most healthcare organizations lack the transactional volume that retailers have, which means that they may have flown 'under the radar' and may not have received pressure to comply with PCI to this point," Burnette said. "As a result, the healthcare industry hasn't matured as quickly with respect to PCI compliance."

You should also ensure that your vendors meet PCI compliance standards when you're utilizing their card processing environments, Burnette advised. Vendors should have a Qualified Security Assessor (QSA)-validated PCI certification for their scope of work. If you're planning to use a vendor to implement a new payment process, ensure that the new payment solution is Point-to-Point Encryption (P2PE)-approved and certified by the **PCI Security Standards Council**.

Resources: To learn more about PCI compliance for healthcare organizations, read Burnette's blog posting at www.lbmcsecurity.com/blog/what-healthcare-organizations-need-to-know-about-pci-31-compliance-for-mobile-payments. Also, check out the PCI Security Standards Council's website at www.pcisecuritystandards.org and see the latest PCI standards guide (Version 3.1) at www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.