Codify
BY AAPC

Health Information Compliance Alert

Reader Questions: Can You Rely On '100% HIPAA Compliant' Products?

Question: Our office has purchased encryption software that claims to be "100-percent HIPAA compliant." When a vendor claims its product is "HIPAA compliant," what does this really mean?

Answer: "Nearly every vendor of an encryption product that targets the healthcare market will claim that the product is HIPAA compliant," stated healthcare attorney **Casey Moriarty** in an April 10 blog posting for Seattle-based **Ogden Murphy Wallace Attorneys.** "This representation is critical because health information that is properly encrypted is exempt from the HIPAA breach notification rules."

Warning: But unfortunately, you cannot buy HIPAA compliance, Moriarty warned. "When a vendor states that its encryption product is 'HIPAA compliant,' the vendor is merely stating that the product meets the HIPAA encryption guidelines for data at rest (stored data) and data in motion (data that is transmitted over networks)."

Just because an encryption product meets HIPAA's data encryption guidelines does not mean that you're ultimately complying with the HIPAA Security Rule simply by using the product. In terms of encryption, the Security Rule standard states that you must "implement a mechanism to encrypt and decrypt electronic protected health information" (ePHI).

What to do: This standard is "addressable," meaning that you must carefully analyze your organization's operations to determine what type of encryption product is "reasonable and appropriate" for your business, Moriarty explained. You must base your analysis on a variety of factors related to your organization, such as:

- Your organization's size, complexity and capabilities;
- Your organization's technical infrastructure, hardware and software security capabilities;
- The costs of encryption measures; and
- The probability and criticality of potential risks to ePHI.

Bottom line: Whether your organization is a small physician office or a large healthcare system, you must document why you believe that a selected encryption product is appropriate for your operations, Moriarty said. "While the idea of buying compliance might be attractive, HIPAA requires covered entities and business associates to look inward and conduct a thorough analysis of their operations."

For more information on HIPAA's data encryption guidelines, go to www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.