Health Information Compliance Alert

Case Study: Don't Be Fooled by Vendors' 'HIPAA-Compliant' Labels

Tip: Investigate BAs' HIPAA track records.

Many vendors target the healthcare market with promises that their products are HIPAA-compliant. Unfortunately, you cannot buy HIPAA compliance - and these claims won't stop the feds from investigating if your organization has a violation or data breach.

Background: In December, the Federal Trade Commission (FTC) announced a settlement with **SkyMed International, Inc.,** a Scottsdale, Arizona-based firm that sells travel and medical emergency services, for exposing consumers' personal information in a data security breach. After a 2019 complaint, the FTC discovered that SkyMed failed to protect individuals' data, including health information, when an unsecured cloud database exposed 130,000 membership records on the internet. In addition, the FTC found that the organization didn't properly assess its risks "by performing penetration testing and other measures, and failed to monitor its network for unauthorized access," an FTC release says.

Though SkyMed alerted current and former customers that their payment and health information wasn't compromised in the breach, the firm didn't actually review the data nor look into unauthorized access of the database materials, the FTC asserts. "Instead, after confirming that the data was online and publicly accessible, SkyMed deleted the database," the release says.

Here's the Case Clincher

But, on top of risk analysis fails, a data breach, and botched investigation of said incident, SkyMed also duped consumers into believing that its services were HIPAA compliant.

"SkyMed deceived consumers by displaying for nearly five years a 'HIPAA Compliance' seal on every page of its website, which gave the impression that its privacy policies had been reviewed and met" HIPAA security and privacy requirements, the FTC alleges.

Many third-party firms say that their products or tools are "HIPAA compliant," but the Department of Health and Human Services (HHS) and its auxiliary agencies don't certify or endorse vendors' products as HIPAA compliant.

Reminder: "HHS does not endorse or otherwise recognize private organizations' 'certifications' regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a 'certification' by an external organization does not preclude HHS from subsequently finding a security violation," HHS Office for Civil Rights (OCR) guidance says.

Find Out What 'HIPAA Compliant' Means to Your Vendor

It's important for covered entities (CEs) and their business associates (BAs) to thoroughly vet their third-party partners and vendors before they enter into business with them. This might involve an initial scorecard to test knowledge of the HIPAA basics, followed by a more comprehensive investigation of their compliance practices, breach history, and incident response protocols.

Why? As required by HIPAA, CEs and BAs must secure patients' protected health information (PHI), and they "would be wise to use caution in evaluating companies that promise 'HIPAA compliance,'" advises attorney **Shannon Hartsfield**, an executive partner with Holland & Knight LLP in Tallahassee, Florida.

"A lot of customers want to see that characterization, and companies selling their services want to provide it. In my view, because HIPAA compliance is an ongoing process, it would be wise to avoid making representations that attempt to ensure 100 percent compliance," Hartsfield says.

Tip: Advertisements that claim products are "HIPAA compliant" or "HIPAA certified" should always be questioned.

"If a healthcare provider is evaluating a company that says they're 'HIPAA compliant,' it would be important to try to get a full understanding of what the vendor means by that," Hartsfield says. "And if a vendor says it's 'HIPPA compliant,' you may need to run the other way! Misspelling HIPAA can be a real red flag," she adds.

End result: According to the proposed settlement, the FTC requires SkyMed to take several actions to correct its compliance issues. Here's a short sampling of what the proposed settlement entails:

- Contact the individuals impacted by the data breach.
- Implement an information security program, including the adoption of a compliance officer, written policies and procedures, and risk analysis and management.
- Ensure security measures are assessed by a third party.

Another component of the settlement relates to SkyMed's "HIPAA-compliant" pledge. "The proposed settlement prohibits misrepresentations about how SkyMed secures consumer information, how it responds to data breaches, and whether the company has been endorsed by or participates in any government-sponsored privacy or security program," notes the FTC release.

Resource: See the case details at www.ftc.gov/system/files/documents/cases/skymed_-_consent_order_ftc_signed.pdf.