Health Information Compliance Alert

Reader Question: What Kind Of Risk Does Using Private Email Accounts Pose?

Question: Our provider group has a secure system for encrypting all outgoing emails from our internal email system. But the physicians are sending protected health information (PHI) from the internal email to their home email (HotMail, Gmail, etc.). Is this putting our company at risk?

Answer: Yes, this is definitely a risky behavior, answers **Jim Sheldon-Dean**, founder and director of compliance services at **Lewis Creek Systems, LLC** in Charlotte, VT. "What happens is those messages wind up on the HotMail or Gmail servers and can wind up being preserved and not really very well protected.

Pitfall: And depending on exactly how you're using HotMail or Gmail, these email providers may even have as part of their terms of service a stipulation that they have a right to look at whatever information that passes through your account, Sheldon-Dean warns. You must try to get the physicians to not use their own personal email accounts, because those email services are not secure.

What's more: Some organizations even report usage of personal unencrypted email accounts as an official breach, Sheldon-Dean adds. "It's up to your attorneys to decide whether that's something you need to report as a breach or not just the fact that [the physicians] have been using those email accounts. So you're certainly in a dangerous situation right now, and you need to consider it very carefully."