Health Information Compliance Alert

You Be The Security Expert: What Do We Do When Our Manager Won't Enforce HIPAA?

Question: What is the duty of a compliance officer whose organization refuses to enforce HIPAA compliance?

Answer: Any employee who is concerned about HIPAA violations should go directly to their compliance officer, experts advise. HIPAA requires that entities develop and distribute a sanctions policy that includes "termination requirements if people fail to abide by the rules," counsels **Stephen Bernstein**, an attorney at **McDermott Will & Emery** in Boston.

If the violation occurs outside the facility, the same rule would apply. "If it's a business associate and we cannot get the problem resolved, our relationship with that business associate would end," explains **Tracie Hanna**, Privacy Coordinator for **American Republic Insurance Company** in Des Moines, IA.

Worst case: If the violator is the compliance officer, don't be afraid to voice your reservations. "Go as high in the organization as you have to," encourages **Michael Hubbard**, an attorney in the Raleigh, NC office of **Smith Anderson Blount Dorsett Mitchell & Jernigan.**

Compliance officers are not immune to HIPAA's regulations, Hanna stresses. "They don't have free rein to do what they want. If they're not abiding by the law, then they have to answer for that," she asserts.

Suggestion: Develop a checks and balances system so that each employee is accountable for their actions, Hanna recommends. **Example:** "We have a HIPAA Steering Committee composed of several senior management members" that makes critical HIPAA decisions and ensures compliance, she confides.

The Bottom Line: The law's the law. Every employee must comply with HIPAA or face termination. "Failure to act [on noncompliance] is a liability and [the ramifications] can go all the way up to the CEO," Bernstein declares.

Remember: If you don't follow your sanctions policy and mitigate noncompliance, **HHS Office for Civil Rights** can come in and penalize!