



Insights

HIPAA Sanction Policies: The Importance of Enforcement

June 3, 2024

By: Stephanie T. Eckerle and Shelley M. Jackson

Covered Entities as defined in the Health Insurance Portability and Accountability Act and its implementing regulations ("HIPAA"), including health care providers and health plans, must have HIPAA policies and procedures in place to protect the privacy and security of patients' protected health information while also ensuring compliance with the right of patients to access their health records. In addition to these important goals, a Covered Entity must establish a sanction policy for members of its workforce who violate the HIPAA policies and procedures, and the sanction policy must be enforced in a consistent manner as to all members of the Covered Entity's workforce.

The Office for Civil Rights ("OCR") recently emphasized the importance of HIPAA policies and procedures, including sanction policies, in its newsletter entitled "How Sanction Policies Can Support HIPAA Compliance" (the "Newsletter"). The Newsletter reminds Covered Entities that failing to implement sanctions when warranted may subject the covered entity to OCR enforcement action.

The Newsletter identified the following important elements to consider in developing and maintaining an effective HIPAA sanction policy:

1. Documenting or implementing sanction policies pursuant to a formal process.
2. Requiring workforce members to affirmatively acknowledge that a violation of the organization's HIPAA policies or procedures may result in sanctions.
3. Documenting the sanction process, including the personnel involved, the procedural steps, the time-period, the reason for the sanction(s), and the final outcome of an investigation.
4. Creating sanctions that are "appropriate to the nature of the violation."
5. Creating sanctions that "vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of protected health information."
6. Creating sanctions that "range from a warning to termination."
7. Providing examples "of potential violations of policy and procedures."



A Covered Entity's sanction policy must be included in its mandatory annual HIPAA audit. OCR's audit protocol includes specific audit requirements related to a Covered Entity's sanction policy to ensure compliance with 45 CFR 164.308 (a)(1)(ii)(B). In addition, OCR states in the Newsletter that "[t]he Privacy Rule's sanction requirement applies only to Covered Entities, not to business associates". Nonetheless, it is wise that business associates, as that term is defined in HIPAA, adopt sanction policies as part of their policies and procedures, as this is a frequent element of compliance set forth in business associate agreements.

Covered Entities should also take steps to ensure its HIPAA policies, including sanction policies, are aligned with its broader Human Resources policies and practices. For example, Covered Entities should review each category of worker to identify the authority by which the sanction policy can be enforced. Some workforce members, such as owners or independent contractors, may require additional scrutiny to ensure applicability and potency of the sanction policy. In addition, Covered Entities should ensure that adequate training and oversight is provided to ensure workers are aware of and agree to comply with applicable HIPAA policies, including sanction policies. Finally, Covered Entities should take steps to ensure an effective and smooth transition, when possible, in the event a HIPAA violation results in termination or other significant sanction and should evaluate the sanction policy in light of applicable local, state, and federal law.

If you have any questions about HIPAA policies and procedures, and specifically how those should be applied to the workforce, contact Stephanie T. Eckerle, Shelley M. Jackson, or your regular Krieg DeVault attorney.

Disclaimer. The contents of this article should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult with counsel concerning your situation and specific legal questions you may have.