Why is a Sanction Policy a “Must Have”?

11/30/2023

Reason #1: The HIPAA Security Rule requires health care providers that are covered entities under HIPAA, and their business associates, to have in place a sanction policy. The policy must require that appropriate sanctions will be applied against members of the workforce who fail to comply with the organization’s HIPPA privacy and security policies and procedures or the requirements of the HIPAA Privacy Rule or Security Rule. When a workforce member violates such policies, procedures or requirements and sanctions are applied, the organization must document the sanctions that are applied, or document a decision not to impose sanctions.

Reason #2: According to the Department of Health & Human Services October 2023 OCR Cybersecurity Newsletter, “Sanction policies can improve a regulated entity’s compliance with the HIPAA Rules.” This is the case because:

“Imposing consequences on workforce members who violate a regulated entity’s policies or the HIPAA Rules can be effective in creating a culture of HIPAA compliance and improved cybersecurity because of the knowledge that there is “a negative consequence to noncompliance enhances the likelihood of compliance.” Training workforce members on a regulated entity’s sanction policy can also promote compliance and greater cybersecurity vigilance by informing workforce members in advance which “actions are prohibited and punishable.” A sanction policy that clearly communicates a regulated entity’s expectations should ensure that workforce members understand their individual compliance obligations and consequences of noncompliance.”

Reason #3: It makes good business sense. Not only can a documented and well-publicized sanction policy have the affect discussed above, but it also may in some cases help shield an employer from liability when terminating an employee for HIPAA infractions. Further, a sanction policy may help reduce or potentially negate governmental penalties that might be imposed as a result of the government’s investigation of a breach incident.

Additional Takeaways: Although HIPAA provides organizations with flexibility in crafting an appropriate sanction policy, plain vanilla sanction policies contained in employee handbooks may not be sufficient to appropriately address HIPAA violations. Organizations should review existing policies and amend or add sanction policies as needed. Such policies should, among other things, (i) establish a formal process for implementing and documenting sanctions; (ii) establish sanctions appropriate to the nature of the violation; and (iii) establish varying degrees of sanction (from warning to termination) depending on the severity of the violation, whether the violation was intentional or unintentional, and whether the workforce member demonstrates a pattern or practice of non-compliance.

Click Here to read the entire November 2023 Healthcare Law Update now!

If you need assistance with your HIPAA compliance program, an OCR investigation, or a data breach incident, please contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com

---