Recognized Security Practices – Take Heed

On January 3, 2020, the Health Information Technology for Economic and Clinical Health (HITECH) Act was amended, creating a "safe harbor" for HIPAA-covered entities and their business associates when potentially facing fines and other penalties under HIPAA. If the covered entity or business associate can "adequately demonstrate" to the Secretary of the U.S. Department of Health & Human Services (DHHS) that it had "recognized security practices" in place for at least the twelve-month period prior to the conduct in question—HIPAA violation, breach event or audit—the Secretary may determine to mitigate any fines to be assessed, favorably terminate early an audit that has been undertaken, or mitigate the remedies in any settlement agreement that may be entered into between the covered entity or business associate and the government. In short, a covered entity or business associate that has experienced a data breach incident and is responding to the related DHHS investigation and document requests, or is otherwise under a HIPAA audit, may be able to assert this safe harbor to reduce or eliminate fines and penalties.

On April 6, 2022, DHHS published a Press Release about its Notice in the Federal Register of the same date security practices. The comment period closed on June 6, 2022, and the remainder of that process is pending. On June 10, 2022, the DHHS Office for Civil Rights (OCR) announced on its list serve that it is producing a pre-recorded video presentation for covered entities and business associates on recognized security practices "to educate regulated entities on the categories of recognized security practices and how entities may demonstrate implementation." OCR indicated the video should be available sometime this summer and that a further announcement will be made.

Covered entities and their business associates should take heed—the government is keenly aware of the cyber crisis created by the endless barrage of cyberattacks targeting the health care industry, and is demonstrating clearly that it intends to scrutinize every business regulated by HIPAA that becomes the subject of a security breach and penalize the non-compliant.

For more information on recognized security practices or for assistance with your HIPAA privacy and security program, contact:

Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com
Carol Grelecki | 973.403.3140 | cgrelecki@bracheichler.com
Vanessa Coleman | 973.364.5208 | vcoleman@bracheichler.com