It's "Personal"– An Expansion of What Qualifies As "Personal Information" Under Pennsylvania's Data Breach Notification Law

By: Debra Weinrich and Amanda McHugh
Cyber Law and Data Protection Alert
12.6.22

In Pennsylvania, data breach notification is governed by the Breach of Personal Information Notification Act ("the Act"). Originally codified in 2005, the Act addresses the security of computerized data and the notification of individuals whose "personal information" was, or may have been, disclosed to unauthorized recipients due to a security system breach, as well as the imposition of penalties for failing to meet the Act's notification requirements. Any entity that "maintains, stores, or manages computerized data that includes personal information" is subject to the Act. The broad scope of the Act applies to everything from state agencies and political subdivisions of the Commonwealth to individuals or businesses of any form (sole proprietorships, partnerships, corporations, associations, etc.) that do business, or destroy records, in Pennsylvania.

Therefore, it is critical for all businesses to understand what qualifies as "personal information" in order to ensure compliance with the Act's post-breach notification requirements. Previously, the Act defined "personal information" as only: (1) a social security number, (2) a driver's license number or state identification number issued in lieu of a driver's license, and (3) a financial account number, credit card number, or debit card number, in combination with a password or security question and answer that would permit access to an online account.

The Pennsylvania Legislature recently took steps to expand the Act's definition of what constitutes "personal information." As a result, three additional types of "personal information" will be subject to the Act's post-breach notification requirements: (1) medical information, (2) health insurance information, and (3) a username *or* email address, *in combination with* a password or security question and answer that would permit access to an online account. The new definition is effective as of May 2, 2023.

"Medical information," pursuant to the Act, includes "[a]ny individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional." Meanwhile, "health insurance information" includes "[a]n individual's health insurance policy number or subscriber identification number in combination with access code *or* other medical information that permits misuse of an individual's health insurance benefit."

Naturally, healthcare providers and entities doing business in the healthcare industry are, and have long been, subject to Federal security and privacy mandates that aim to protect an individual's personal health information via, at least, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and the associated regulations. In its recent amendment of Pennsylvania's Breach of Personal Information Notification Act, the state legislature acknowledged HIPAA's pre-existing requirements by explicitly carving an exception into the Act's post-breach notification requirements. The Act now provides that any entity that is subject to HIPAA will be deemed in compliance of the Act's notification requirements so long as the entity is in compliance with HIPAA's privacy and security standards for the protection of electronic personal health information.

Finally, regarding data breaches involving an individual's username or email address, the Act now clarifies that post-breach electronic notification is permissible so long as the notice provides specifically enumerated direction regarding the steps needed to be performed to mitigate the potential impact of the breach. The electronic notification must include "direction to the affected individual to promptly change their password and security question or answer, or to take other steps appropriate to protect their online account."

While the amendments do not affect those in the healthcare field in a particularly meaningful manner, businesses not subject to HIPAA who do business in Pennsylvania need to be cognizant of the expanded definitions. They should review their computer network security systems, policies, practices and training programs to ensure they are taking steps to attempt to prevent data breaches. Ultimately, a related update is recommended to assist with compliance if an applicable breach of personal information occurs.

If you have questions or would like additional information, please contact Debra Weinrich (weinrichd@whiteandwilliams.com; 215.864.6260) or Amanda McHugh (mchugha@whiteandwilliams.com; 215.864.6332).

This correspondence should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only and you are urged to consult a lawyer concerning your own situation and legal questions.