The PIOGA Press

March 2024 • Issue 167

Developments in Data Privacy

Article provided by Babst Calland - Authors: Ember K. Holmes and Justine M. Kasznica

In 2023, Pennsylvania's Breach of Personal Information Notification Act (BPINA), underwent its first major update since it was signed into law in June 2006. The Amended BPINA[1] went into effect on May 2, 2023. The Amended BPINA affects all Pennsylvania entities that store information belonging to Pennsylvania residents, including energy companies, but has the most significant impact on state agencies and entities that contract with state agencies.

BPINA was designed to set security parameters and standards for entities that maintain, store, or manage computerized data containing the Personal Information (as defined below) of Pennsylvania residents. BPINA sets forth specific requirements for notifying residents of security system breaches. The Amended BPINA creates new definitions for previously undefined terms in BPINA, amends existing term definitions, and bolsters notification and security requirements for state agencies, state agency contractors, counties, public schools, and municipalities.

As a state agency, the Pennsylvania Department of Environmental Protection (PADEP) will be subject to this higher level of scrutiny with regard to its handling of personal information. In addition, any entity that contracts with the PADEP or maintains data on behalf of the PADEP or any other state agency is also subject to these more stringent requirements and should be familiar with the updates as applicable to their notification, reporting, and encryption practices.

1 Breach of Personal Information Notification Act-Omnibus Amendments, Act of Nov. 3, 2022, P.L. 2139, No. 151.

Expanded Definition of "Personal Information" and Related Notification Requirements

- The original BPINA definition of "Personal Information" included: (i) social security numbers; (ii) driver's license numbers or state identification card numbers issued in lieu of driver's licenses; and (iii) financial account numbers and credit or debit card numbers, in combination with any required access codes or passwords that would permit access to an individual's account.
- The Amended BPINA expands "Personal Information" to include medical information, health insurance information, and username or email address information in combination with a password or security question. This change applies to all entities that collect and store information of Pennsylvania residents and will most significantly impact companies that contract with third-party vendors to provide services such as online payments, health portals, and banking. These services almost always involve use of a username and password, and exposure of this information will now trigger response and notification protocols.
- The Amended BPINA also added "electronic notice" as a valid means of notifying individuals that their information may have been materially compromised. This can be accomplished by directing the individual to promptly change their password and security question or take any other steps that may be appropriate to protect their information.

Notification and Security Requirements for State Agencies, State Agency Contractors, Counties, Public Schools, and Municipalities

- With regard to state-related entities, the

Amended BPINA redefines the scope of notification requirements and imposes a variety of heightened, new notification requirements on these entities. The term "State Agency Contractor" is defined for the first time as "a person, business, subcontractor, or third-party subcontractor that has a contract with a state agency for goods or services that require access to personal information for the fulfillment of a contract."

- Under the Amended BPINA, entities that maintain, store, or manage computerized data containing Personal Information on behalf of the Commonwealth are required to utilize encryption or other adequate security measures to protect Personal Information from view or access by an unauthorized party. These entities must also maintain a policy governing encryption or other security measures, and a policy relating to data storage and retention.

Federal Regulation Compliance

- The Amended BPINA provides a "safe harbor" for entities, state agencies, and state agency contractors that comply with federal notification requirements imposed by a functional federal regulator – such entities are deemed to be compliant with BPINA. For example, any entity that is subject to and in compliance with the privacy and security standards under the Health Insurance Portability and Accountability Act of 1996[2] (HIPAA) or the Health Information Technology for Economic and Clinical Health Act[3] (HITECH) are deemed to be compliant with the Amended BPINA.
- The Amended BPINA also provides that any entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary state or functional federal regulator is deemed to be compliant with the Amended BPINA. Entities that are not currently in compliance with any such federal requirement must actively ensure compliance with the BPINA.

Next Steps

- All entities that do business in Pennsylvania, maintain data belonging to Pennsylvania residents, or do business with the Commonwealth or its agencies, should familiarize themselves with the new requirements, and should review their security-related policies, practices, and incident response plans to ensure compliance with the Amended BPINA.
- Violations of the Amended BPINA are considered unfair or deceptive acts under Pennsylvania's Unfair Trade Practices and Consumer Protection Law and the penalties for violations may be injunction, restitution, or other civil penalties.

2 Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (Aug. 21, 1996).

3 Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, Title XIII (Feb. 17, 2009).