ECKERT SEAMANS ATTORNEYS AT LAW

November 8, 2022

Data Privacy & Security Alert

Pennsylvania Amends its Breach of Personal Information Notification Act

By Matthew H. Meade and Emma M. Lombard

On November 3, 2022, Governor Tom Wolf approved Senate Bill 696, which is An Act Amending P.L. 474, Pennsylvania's Breach of Personal Information Notification Act. The Act becomes effective 180 days after its enactment, which will be **May 2, 2023**.

The Act amends the existing data breach notification law to expand the categories of "personal information" for which notice is required, provides new definitions for previously undefined key terms, drastically reduces the time for individual notifications by state entities, and imposes new reporting requirements on state agencies, state agency contractors, counties, public schools, and municipalities. The Act further requires state-related entities to utilize encryption and implement security-related policies.

Notification Obligations for All Entities

The Act expands the definition of "Personal Information" by including the following:

- "**Medical information**," which is defined as "Any individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a healthcare professional."
- "**Health insurance information**," which is defined as "An individual's health insurance policy number or subscriber number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits."
- "Username or e-mail address, in combination with a password or security question that would permit access to an online account"

When listed in combination with a Pennsylvania resident's first and last name, any of these protected data elements will require notification if there has been a breach of the security system as defined under the law. Businesses and other organizations that are not subject to HIPAA but maintain health information about Pennsylvania residents will soon need to evaluate a cyber incident to determine whether the amended Pennsylvania law applies.

Notification Obligations for State Entities

Though the Act retains the same individual notification obligations for non-state entities, which requires notice be provided "without unreasonable delay," the Act critically re-defines the scope of individual and regulator notification obligations for state-related entities. Under the Act:

- A State agency, defined as "Any agency, board, commission, authority or department of the Commonwealth and the General Assembly" must now provide notice to individuals within **seven business days** following the **determination** of a breach, and concurrently provide notice to the Office of the Attorney General.
    - A State agency under the Governor's jurisdiction must also provide notice of the breach to the Governor's Office of Administration within **three business days** following the **determination** of a breach.

- A county, public school, or municipality must provide notice to individuals within **seven business days** following the **determination** of a breach and must provide notice to the District Attorney in the county where the breach occurred within **three business days** following the **determination** of a breach.
    - "Public school" means any school district, intermediate unit, charter school, cyber charter school, or area career and technical school.
- A state agency contractor, defined as "A person, business, subcontractor, or third-party subcontractor that has a contract with a state agency for goods or services that requires access to personal information for the fulfillment of the contract" must now provide notice to the Chief Information Security Officer, or a designee of the State Agency, as soon as reasonably practicable after the **discovery** of a breach.

The Act further provides definitions for "determination" and "discovery," which inform the operative timeline for an entity's notification obligations above. "Determination" is defined as "A verification or reasonable certainty that a breach of the security of the system has occurred." "Discovery" is a new defined term and means "The knowledge of or a reasonable suspicion that a breach of the system has occurred." The newly added definition of "Discovery" makes clear that a vendor or a state contractor must provide notice of a breach to the entity or state entity for whom it maintains data when it knows or has a reasonable suspicion of a breach. The Act also provides that notification may be delayed "in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system."

Security Obligations for State Entities

The Act also requires that entities who maintain, store, or manage computerized data on behalf of the Commonwealth that constitutes Personal Information to utilize encryption, or other appropriate security measures, to reasonably protect the transmission of Personal Information over the internet from being viewed or modified by an unauthorized third party. The same entities must develop and maintain: (1) a policy to govern the encryption or other security measures; and (2) a policy for data storage and retention.

Next Steps for State Entities

In sum, the Act will require state agencies, counties, municipalities, and public schools to notify individuals whose Personal Information is compromised because of a security breach within seven business days of the entity verifying or becoming reasonably certain that a breach has occurred. At the same time, state agencies must provide notice to the Office of the Attorney General. Counties, municipalities, and public schools, by contrast, must provide notice to the county District Attorney within three business days of the determination of a breach.

As a practical matter, the "determination" of a breach does not occur at the same time as the "discovery" of a breach. The determination of a breach often requires input from forensic analysts and attorneys, and while entities facing these new reporting requirements should be prepared to comply with them, state-related entities can take several preventative measures now to better position themselves for compliance when the Act becomes effective. This includes updating incident response plans, reviewing data retention practices, and implementing or revising existing policies for data transmission and retention.

Next Steps for All Entities

In addition to updating incident response plans, this new law emphasizes the need to evaluate the personal information maintained by the organization and regularly practice responding to cyber incidents through tabletop exercises, especially for entities subject to the seven-day notification period.

ECKERT SEAMANS
ATTORNEYS AT LAW