Pennsylvania Data Breach Notification Act Amendment: What Businesses Need to Know for May 2, 2023

Related Attorneys

Michael P. Oliverio

Robert D. Shope

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 4.26.2023

Pennsylvania' Breach of Personal Information Notification Act, P.L. 474 (the Act) has been in place since June 2006. The Act generally defines what constitutes "personal information" and requires companies in Pennsylvania that become aware of a data breach involving personal information to provide notice of to the individuals whose data may have been exposed.

On November 3, 2022, Governor Tom Wolf approved Senate Bill 696 (the Amendment), which becomes effective on ***May 2, 2023***. The Amendment is the first major update to the Act, and contains significant changes worth noting for all businesses that store personal information on Pennsylvania residents. The Amendment is of particular importance for companies that contract with state agencies.

Key Points

The Amendment's key aspects for all businesses are:

- Expanding the categories of "personal information" under the Act;
- Defining key terms in the Act that were previously undefined;
- Permitting electronic notice to affected individuals, under certain circumstances;
- Providing an expanded safe harbor for entities that comply with the breach notification rules imposed by a functional federal regulator, or a primary regulator in another state.

In addition to these general requirements, the Amendment includes significant new rules for state agencies, counties, public schools, and other municipal entities, as well as companies that contract with state agencies (referred to as state agency contractors):

- Requiring state agencies to report data breaches to both affected individuals and the Attorney General's office within seven business days;

- Requiring state agency contractors to report data breaches to their relevant state agency as soon as practicable, and in any event no later than required under the relevant contract;
- Requiring state agencies under the jurisdiction of the Governor to additionally report breaches to the Governor's Office of Administration within three business days;
- Requiring state agencies entering into new contracts with state agency contractors to include terms ensuring compliance with the Act;
- Providing a safe harbor for state agencies and state agency contractors that have a primary state or federal regulator, so long as they comply with those regulations;
- Requiring Pennsylvania counties, public schools, and other municipal entities to report data breaches to affected individuals within seven days, and to the District Attorney in the relevant county within three business days.

Finally, the Amendment requires any entity that maintains, stores, or manages computerized data on behalf of the Commonwealth to utilize encryption, or other appropriate security measures, to protect the data. Such entities must also develop and implement a policy to govern the security of such data, including in storage and transmission. Entities must review such policies at least annually, and update them as needed.

Amendment Deep Dive

Definitions:

1. "Personal Information" modified

Types of information currently included within the Act's definition of "Personal Information" include (i) social security numbers, (ii) driver's license numbers or state identification card numbers issued in lieu of a driver's license, and (iii) financial account numbers, credit or debit card numbers, in combination with any required access codes or passwords that would permit access to an individual's financial account.

The Amendment expands this list to include: iv) medical information, (v) health insurance information, and (vi) a username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

"Health Insurance Information" is defined as "[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 benefits."

"Medical information" is defined as "[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."

2. "State Agency Contractor" added

The newly defined term, “State Agency Contractor” provides “[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.”

3. “Discovery” and “Determination” added

The newly defined term, “Discovery”, provides “[t]he knowledge of or reasonable suspicion that a breach of the security of the system has occurred.” Compare this to the narrower term, “Determination”, which provides “[a] verification or reasonable certainty that a breach of the security of the system has occurred”.

These new definitions play an important role in the Act, as disclosure responsibilities in most cases begin to run from the “Determination” of a breach, but in certain instances will now begin to run upon “Discovery” instead.

New Notice Requirements

The Amendment maintains the “general rule” that “an entity that maintains, stores or manages computerized data that includes personal information” must provide notice of a data breach “without unreasonable delay.” However, the Amendment carves out more stringent notice requirements for “state agencies” and “state agency contractors”, as defined.

1. State Agency

A state agency that “determines that it is the subject of a breach of the security of the system affecting personal information maintained by the state agency or state agency contractor” shall provide notice of the breach “within seven business days following determination of the breach of the security of the system.” Notification must also be made concurrently by state agencies to the Pennsylvania Office of the Attorney General. A county, public school or municipality that is the subject of a breach must also notify their district attorney within three business days following "determination" of the breach.

Here, we see the new definition of “determination” being used. Under that definition, the deadline for state agencies to make disclosure runs from the moment that it has “verified” or reached “reasonable certainty” that a data breach has occurred.

2. State Agency Contractors

As for a “State Agency Contractor,” the Act requires that it:

> *“shall, upon discovery of the breach of the security of the system, notify the chief information security officer, or a designee, of the State agency affected by the State agency contractor's breach of the security of the system as soon as reasonably practical, but no later than the time period specified in the applicable terms of the contract between the State agency contractor and the State agency of the breach of the security of the system.”*

It is important to note that the disclosure trigger for state agency contractors is NOT the “Determination” standard discussed above. Instead, state agency contractors are obligated to disclose to their state agency upon “Discovery” of a breach. This means that the trigger for state agency contractors begins to run as

soon as the contractor gains "knowledge of or reasonable suspicion" that a breach has occurred. Compared to the definition of "Determination," the "Discovery" standard appears to mandate disclosure earlier in the process, in a broader set of cases, where there is suspicion of a possible data breach, but before the breach has been "verified."

An important question for state agency contractors will be how the Amendment impacts existing contracts that may not address data breach and disclosure obligations. The Amendment's trigger date is May 2, 2023, and applies to any data breach that occurs on or after that date. Accordingly, the date of the contractor's contract with the state agency does not appear to be relevant as to whether the contractor is obligated to disclose.

Companies with contracts with state agencies will want to examine their agreements on a case-by-case basis, and seek guidance from legal counsel and/or the state agency on how the Amendment affects existing contractual duties. In the future, the Amendment requires all state agency contracts to require compliance with the Act, so contractors dealing with state agencies should expect to see updated cyber security and data breach terms in government contracts moving forward.

Permitted Forms of Notice

The Act has always permitted notice to affected individuals via written notice, telephonic notice, or email (so long as a prior business relationship exists and the entity has a valid email address). The Act has also previously permitted "substitute notice" in cases of large breaches, which required notice via email, posting on the entity's website, and notification to major statewide media.

The Amendment expands the definition of "Notice" under the Act to permit "Electronic notification" in situations where the breach has exposed user names, passwords, and/or security questions. This type of notice is available in situations where a breach involves "personal information for a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account" and/or other accounts for which the same username and password apply. Electronic notice for this type of breach is appropriate so long as the notice directs the affected individual to promptly change their password and security questions, or "take other steps appropriate to protect" the individual's online account(s).

Data Security Policy Requirements for the Commonwealth

The Amendment adds a new section to the Act, requiring that "[a]n entity that maintains, stores, or manages computerized data on behalf of the Commonwealth that constitutes personal information shall 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 new section of the Act also requires such entities to "develop and maintain" policies governing both transmission of data and storage of data, to reduce the risk of future data breaches. These policies must be reviewed at least annually and updated as necessary.

The Amendment includes a carve-out from these new data security policy requirements for entities (and their business associates) that are subject to, and comply with, the privacy and security standards under HIPAA and HITECH. Accordingly, entities that maintain Commonwealth data that are subject to HIPAA

and/or HITECH, will not have to wrestle with additional or conflicting obligations under the Pennsylvania Act.

Compliance Safe Harbor

The Act currently deems entities that comply with federal notification requirements imposed by a functional federal regulator, as being in compliance with the Act. The Amendment expands this existing safe harbor. First, the Amendment expands the safe harbor to apply to "entit(ies), a state agency, or a state agency's contractor." Second, the safe harbor now applies to entities, state agencies, and state agency contractors who comply with either federal notification requirements imposed by a functional federal regulator, but also requirements imposed by the entity's "primary State" regulator.

The exact implications of this expanded safe harbor are not clear at this time, due to the use of "primary State regulator," a term that is not otherwise defined. As relevant Pennsylvania stakeholders provide further guidance, hopefully businesses and the legal community will get clarification. Businesses that operate in multiple states, that already comply with a general data security and breach notification law imposed by another state, would welcome a broad interpretation of the safe harbor.

Key Takeaways

Pennsylvania's first major update to its 2006 Breach of Personal Information Notification Act expands the categories of data covered as "personal information" and imposes stringent notice requirements on state agencies, state agency contractors, and municipal entities. It also imposes new data security policy requirements on any "entity" that maintains, stores, or manages computerized data on behalf of the Commonwealth. Companies that do business in Pennsylvania, maintain data on Pennsylvania residents, or that do business with the Commonwealth or state agencies, should review the Amendment to ensure they are in compliance on or before the May 2, 2023, compliance date. If you have questions about data protection and disclosure obligations under Pennsylvania law, contact your Vorys lawyer.