POLSINELLI

Publications

September 16, 2026 • Updates

Delaware Data Breach Notification Law Amendment Adds Earlier AG Notice, Narrows GLBA and HIPAA Safe Harbor

Key Updates

- Delaware enacted HB 381 on Sept. 2, which amends the state's data breach notification law by adding an early Attorney General reporting requirement when an organization cannot identify affected Delaware residents within 60 days.
- HB 381 also narrows an existing compliance safe harbor for GLBA-regulated financial institutions and HIPAA-regulated entities, meaning those entities may need to reevaluate their obligations under Delaware's breach notification law.

Why It Matters

- Organizations that maintain the personal information of Delaware residents may need to evaluate notifying the Delaware Attorney General before completing individual notifications, particularly when forensic investigation or data review extends beyond Delaware's 60-day notice period. Certain regulated entities can no longer rely on a broad safe harbor under state law.

Next Steps

- Incident response teams should update notification matrices, escalation procedures and breach-response workflows to account for Delaware's early Attorney General reporting trigger, substitute notice requirements, and narrower regulated entity safe harbor.

On Sept. 2, Delaware Governor Matt Meyer signed House Bill 381 (HB 381), which took effect immediately and amended Delaware's data breach notification law. HB 381 creates an early Attorney General reporting requirement when an organization cannot identify particular affected Delaware residents within 60 days after determining a data breach has occurred, adds Attorney General notice to Delaware's substitute notice process, and narrows the safe harbor for GLBA-regulated financial institutions and HIPAA-regulated entities. Organizations maintaining personal information about Delaware residents should update their incident response plans to reflect the new requirements.

Related People

- Alexander D. Boyd

Related Capabilities

- Privacy & Cybersecurity

How Does HB 381 Change the Requirement to Notify the Delaware Attorney General of a Data Breach?

Existing Delaware law generally requires organizations to notify the Delaware Attorney General of data breaches involving notice to more than 500 Delaware residents. The notice must take place no later than when the organization notifies the residents.

Delaware also generally requires notice to affected residents without unreasonable delay and within 60 days after determining that a data breach occurred. If, despite reasonable diligence, an organization cannot identify within that period that the personal information of particular Delaware residents was included, it must notify those residents as soon as practicable after making that determination.

Now, if despite reasonable diligence an organization cannot identify within 60 days that the personal information of particular Delaware residents was included in the breach, the organization must notify the Delaware Attorney General within the original 60-day period after determining that the breach occurred. For data incidents involving complex forensic investigations and data review, this early Attorney General notice may be required even though notices to individuals may not occur until a later time. This new early Attorney General requirement is similar to laws in states such as Texas and Vermont, which impose separate regulatory reporting deadlines that may precede completion of individual notice.

HB 381 also makes Attorney General notice part of Delaware's substitute notice process.

Does HB 381 Eliminate Delaware's 500-Resident Threshold for Attorney General Notice?

No. HB 381 does not amend Section 12B-102(d), which continues to require Attorney General notice when the number of Delaware residents to be notified exceeds 500. The new early reporting and substitute notice requirements operate in addition to that existing requirement.

However, some public legislative statements about HB 381 create uncertainty in this area. The sponsors described HB 381 as requiring businesses to notify the Attorney General within 60 days and as helping ensure the office receives information about all breaches that may contain sensitive data. Because that description is broader than the enacted text, organizations should monitor guidance from the Delaware Attorney General's Office.

What Does HB 381 Mean for Organizations Regulated by HIPAA or the GLBA?

Previously, an organization that maintained breach procedures established by its primary or functional regulator and notified affected Delaware residents under those procedures was deemed compliant with Chapter 12B as a whole. HB 381 limits that deemed compliance to Section 12B-102(c), which governs the timing of individual notice and contains the new 60-day Attorney General requirement for situations when an organization cannot identify within that period that the personal information of particular Delaware residents was included in the breach.

Under the narrower safe harbor, these regulated organizations need to reevaluate their obligations under Delaware law. In particular, regulated organizations must now separately evaluate compliance with Delaware's Attorney General notification requirement for breaches requiring notice to more than 500 Delaware residents and Delaware's credit monitoring requirement for certain breaches involving Social Security numbers.

Although the revised safe harbor applies to the new 60-day Attorney General requirement, regulated entities must continue to evaluate their early regulator notification obligations under federal law, including the FTC's data breach notification rule for certain nonbank financial institutions, the NCUA's 72-hour cyber incident reporting rule and the federal banking regulators' 36-hour notification requirement for certain notifiable computer security incidents.

What Should Organizations Do Now?

Organizations maintaining information about Delaware residents should revise their incident response plans to incorporate the broader Attorney General notification requirements and narrower regulated entity safe harbor. This amendment serves as a reminder to incorporate the varying forms of early regulator notice into the incident notification process and not to wait until the investigation and data review are complete before evaluating regulator notification obligations.

HB 381 also highlights the increasingly complicated interaction between state breach notification statutes and sector-specific regulatory requirements. Organizations should not assume that compliance with their primary regulator's breach procedures necessarily satisfies all applicable state law requirements.

For more information about Delaware HB 381, state and federal data breach notification requirements, or incident response preparedness, contact Polsinelli's Privacy and Cybersecurity team.