How does Cyber Crucible support Pennsylvania's breach-notification law?

Short answer: Pennsylvania's Breach of Personal Information Notification Act (73 P.S. §2301, as amended by Act 151 of 2022) requires notifying affected residents — and, for larger breaches, the Attorney General — after a breach of covered personal information. Cyber Crucible supports a Pennsylvania organization's obligations by holding no personal information itself and by providing prompt, evidence-grade incident information so the organization can meet its statutory timelines. Cyber Crucible is headquartered in Pittsburgh, Pennsylvania.

How it aligns

- **No personal information held** — the organization retains control of any breach determination and notice; there is no vendor-side data set to lose.
- **Prompt incident information** — the breach-response process is built to give the organization the facts it needs to notify within the required timeframe.
- **Expanded definitions handled** — the 2022 amendment broadened covered personal information (including medical and certain credential combinations); the no-collection design keeps Cyber Crucible clear of those categories.

Vendor-selection notes

For breaches affecting more than 500 Pennsylvania residents, the amendment adds Attorney General notice; Cyber Crucible's role is to support, not to determine, that obligation. Incident-handling detail is available under NDA.

Revision #2
Created 2026-07-23 15:18:43 UTC by Dennis Underwood
Updated 2026-07-23 18:20:09 UTC by Dennis Underwood