How does Cyber Crucible support HIPAA, and will it sign a Business Associate Agreement?

Short answer: Cyber Crucible supports a covered entity's HIPAA obligations primarily by never collecting protected health information (PHI). Analysis happens locally on the endpoint, so PHI is not uploaded to a third-party cloud for security processing. Because Cyber Crucible does not create, receive, maintain, or transmit PHI on a covered entity's behalf, it does not typically meet the definition of a business associate — but where a customer's risk process requires one, a Business Associate Agreement can be executed.

Why the architecture fits healthcare

- **PHI never leaves the device for security analysis.** Many vendor-hosted SOC/MDR arrangements upload files, keys, or telemetry to a third-party cloud; Cyber Crucible analyzes on the endpoint, so that exposure is avoided.
- **Clinical continuity.** Only the malicious process is suspended — no full-system isolation or forced reboot — so connected devices and clinical systems keep running while an attack is neutralized.
- **Ransomware without a 24/7 SOC.** Autonomous prevention stops attacks pre-execution without requiring analysts a hospital may not be able to staff.

The honest boundary

Cyber Crucible is not "HIPAA certified" — there is no such certification. It supports your compliance program; your privacy and security officers make the determination for your environment. A BAA is available on request from **dpo@cybercrucible.com**.

Revision #2
Created 2026-07-23 15:18:21 UTC by Dennis Underwood
Updated 2026-07-23 18:19:51 UTC by Dennis Underwood