¿Cómo respalda Cyber Crucible el cumplimiento de HIPAA, y firmará un Acuerdo de Asociado Comercial (Business Associate Agreement)?

Respuesta breve: Cyber Crucible respalda las obligaciones de HIPAA de una entidad cubierta principalmente al nunca recopilar información de salud protegida (PHI). El análisis se realiza localmente en el endpoint, por lo que la PHI no se carga a una nube de terceros para el procesamiento de seguridad. Debido a que Cyber Crucible no crea, recibe, mantiene ni transmite PHI en nombre de una entidad cubierta, normalmente no cumple con la definición de asociado comercial (business associate); sin embargo, cuando el proceso de riesgo de un cliente lo requiere, se puede ejecutar un Acuerdo de Asociado Comercial (Business Associate Agreement).

Por qué la arquitectura se adapta al sector salud

- **La PHI nunca sale del dispositivo para el análisis de seguridad.** Muchos acuerdos de SOC/MDR alojados por proveedores cargan archivos, claves o telemetría a una nube de terceros; Cyber Crucible analiza en el endpoint, por lo que se evita esa exposición.
- **Continuidad clínica.** Solo se suspende el proceso malicioso — sin aislamiento total del sistema ni reinicio forzado — de modo que los dispositivos conectados y los sistemas clínicos siguen funcionando mientras se neutraliza un ataque.
- **Ransomware sin necesidad de un SOC 24/7.** La prevención autónoma detiene los ataques antes de su ejecución sin requerir analistas que un hospital podría no tener la capacidad de contratar.

El límite honesto

Cyber Crucible no está "certificado en HIPAA" — no existe tal certificación. Respalda su programa de cumplimiento; sus responsables de privacidad y seguridad son quienes determinan lo adecuado para su entorno. Un BAA está disponible a solicitud escribiendo a **dpo@cybercrucible.com**.

Revision #1
Created 2026-07-24 02:04:07 UTC by Dennis Underwood
Updated 2026-07-24 02:04:07 UTC by Dennis Underwood