How your data is protected.

FOR YOUR IT OR COMPLIANCE TEAM · UPDATED JUNE 2026

To build your briefing, Dermhilda works with the data your practice already keeps in ModMed — and treats every bit of it as protected health information, because that's what it is. A Business Associate Agreement is in place before any of it is touched. That comes first, always.

From there, the posture is built in layers, on the deliberate assumption that any single safeguard can fail and the rest should still hold. HIPAA sorts those safeguards into three kinds — technical, physical, and administrative — and so do we.

TECHNICAL SAFEGUARDS

The digital controls

- Patient data is encrypted at every stage — AES-256 at rest, and encrypted in transit across a private, zero-trust network with no public-facing way in.
- Every entry point requires verified-push multi-factor authentication. Access follows the HIPAA “minimum necessary” standard and is tied to a named person — no shared logins.
- Endpoints are monitored continuously, with behavioral threat detection that can isolate a compromised device on its own.
- Patient data is never stored on the machines our team works from; the work happens inside our secured environment, and temporary working data is wiped on a fixed schedule rather than left to accumulate.

PHYSICAL SAFEGUARDS

The hardware

- The systems that process patient data sit in a private, access-controlled location in the United States.
- Drives are hardware-encrypted and keyed to the machine they're in, so a stolen disk can't be read anywhere else.
- Retired hardware is cryptographically wiped or physically destroyed to the NIST 800-88 standard.

ADMINISTRATIVE SAFEGUARDS

The program around it

- A formal HIPAA security risk assessment every year, documented as a system of record.
- A Business Associate Agreement with every infrastructure provider that touches the data — Google Cloud, Microsoft, Paubox, iDrive — audited annually.
- Access is reviewed and recertified on a fixed cycle, and offboarding revokes it within the hour.
- Annual HIPAA and security-awareness training for everyone, required to keep access — with records retained for six years.

That's the posture, top to bottom. Bring your toughest questions — and your IT or compliance people — and we'll answer them directly, with documentation where it matters.