[Type here]

JANUARY 31, 2026

DBT

DIRECT BUSINESS TECHNOLOGIES

PART 2 + HIPAA ALIGNMENT COMPLIANCE CHECKLIST

IT / CYBERSECURITY

JUSTIN MIRSKY
DBT SUPPORT
Louisville, KY

1) Data discovery + scope (you can’t secure what you can’t find)

- ☐ Identify **where Part 2/SUD data exists** (EHR modules, document management, shared drives, email, patient portals, data exports, backups, archives).
- ☐ Map **data flows**: ingestion → storage → access → sharing (internal + external).
- ☐ Confirm **systems of record** and “shadow IT” locations (scanned PDFs, fax ingestion, provider inboxes, local device caches).
- ☐ Inventory **integrations** touching SUD data (HL7/FHIR interfaces, labs, billing, CRM, intake tools, telehealth).

2) Identity, authentication, and access control (least privilege with evidence)

- ☐ Enforce **MFA for all users** accessing systems that contain ePHI/Part 2 data (including remote access, admin access, and web portals).
- ☐ Implement **role-based access** and review roles for “excess access.”
- ☐ Require **privileged access management** or at minimum separate admin accounts + strong controls.
- ☐ Quarterly (or better) **access reviews** for:
  - clinical staff
  - billing
  - IT/admins
  - vendors and contractors
- ☐ Ensure **termination/offboarding** removes access quickly (same day or automated).

3) Logging, audit trails, and monitoring (OCR cares about this)

- ☐ Verify audit logging is enabled on:
  - EHR / practice management
  - identity provider / directory
  - servers and endpoints
  - firewall/VPN/SASE/ZTNA
  - email security
  - cloud apps where SUD data is stored/transmitted
- ☐ Centralize logs into SIEM (or equivalent) with retention aligned to policy.
- ☐ Alerting for key events:
  - unauthorized access attempts / brute force
  - new admin accounts / privilege escalation

  - mass export/download activity
  - anomalous logins (geo/time/device)
  - audit logging disabled / tampering
- ☐ Document **who reviews alerts** and **what happens next** (SOP + ticket trail).

4) Risk analysis + risk management (ongoing, not "one and done")

- ☐ Perform a **security risk analysis** that explicitly includes Part 2 systems and flows.
- ☐ Maintain a **risk register** with:
  - risk statement
  - affected systems
  - likelihood/impact
  - compensating controls
  - remediation owner + due date
- ☐ Establish a cadence: at least annually + on major changes (new EHR module, cloud migration, vendor switch).

5) Endpoint + server security baseline (practical controls)

- ☐ Patch management SLAs (OS + third-party) with reporting.
- ☐ EDR/AV deployed and monitored; tamper protection enabled.
- ☐ Disk encryption for endpoints and portable media controls.
- ☐ Secure configuration baseline (CIS-aligned where feasible).
- ☐ Local admin rights minimized; application control where appropriate.

6) Email + collaboration controls (common breach path)

- ☐ Strong phishing protections (DMARC/SPF/DKIM, filtering, sandboxing).
- ☐ Conditional access where possible (device compliance / MFA enforcement).
- ☐ DLP or at least controls around forwarding and external sharing for sensitive data.
- ☐ External sharing restrictions for cloud drives (SharePoint/OneDrive/Google Drive).

7) Vendor / Business Associate controls (this is where many get burned)

- ☐ Confirm BAAs are in place for all vendors touching Part 2/ePHI data.
- ☐ Validate vendor security posture: MFA, logging, breach notification process, encryption.
- ☐ Ensure contracts address:
  - incident notification timelines
  - subcontractor controls
  - right to audit / evidence upon request

- ☐ Track vendor access (who/what/when) and remove stale accounts.

8) Incident response + breach readiness (test it)

- ☐ Incident Response Plan includes Part 2/ePHI scenarios.
- ☐ Tabletop exercise at least annually (phishing → mailbox compromise → data exfil).
- ☐ Clear internal escalation: IT → compliance → leadership → legal → insurer.
- ☐ Evidence collection plan (logs, endpoint isolation, chain of custody).
- ☐ Breach notification workflow and contact list maintained.

9) Backups + resilience (availability is part of security)

- ☐ Immutable/offline backup strategy for ransomware resilience.
- ☐ Restore tests performed and documented.
- ☐ Separation of duties and access controls around backup systems.

10) Policy + documentation (what you'll need if audited)

- ☐ Policies updated (access control, logging, IR, risk mgmt, vendor mgmt).
- ☐ Procedures match reality (screenshots/config evidence helps).
- ☐ Training records maintained (security awareness + role-based training).
- ☐ Evidence repository: where logs/reports/tickets live and how to retrieve them quickly.