COVERED ENTITIES & BUSINESS ASSOCIATES

HIPAA Security Rule Checklist

There's no such thing as a "HIPAA certificate." What a regulator wants is a documented risk analysis and safeguards that are actually running - the three families below, plus the paperwork that ties them together. The full page: **www.crccloud.com/services/compliance/hipaa/**

Administrative safeguards

- ☐ **A documented risk analysis of where ePHI lives and how it's exposed**
  the foundation of the whole program.
- ☐ **Assigned security responsibility**
  a named person accountable.
- ☐ **Workforce security-awareness training, refreshed regularly.**
- ☐ **A contingency plan: backup, disaster recovery, and emergency-mode operation.**

Physical safeguards

- ☐ **Facility access controls for where systems and ePHI live.**
- ☐ **Workstation and device use policies.**
- ☐ **Media controls for disposal and re-use of devices that held ePHI.**

Technical safeguards

- ☐ **Access control with unique user IDs and automatic logoff.**
- ☐ **Audit controls**
  logging of who accessed ePHI and when.
- ☐ **Integrity controls so ePHI isn't improperly altered or destroyed.**
- ☐ **Transmission security**
  encryption of ePHI in transit.
- ☐ **Encryption of ePHI at rest**
  "addressable," which in practice means required unless you can document why not.

The paperwork that ties it together

- ☐ **A signed Business Associate Agreement (BAA) with every vendor that touches ePHI.**
- ☐ **Written policies and procedures you can produce for an OCR inquiry.**
- ☐ **Documentation kept current**
  an audit meets a binder, not a scramble.

CRC Cloud operates the technical safeguards this program stands on - MFA, encryption, SIEM audit logging, awareness training and Microsoft 365 backup - inside Secure IT, which is the floor for a covered entity. Core IT is not an option for a regulated environment.