HIPAA Requirements

The HIPAA Privacy and Security Rule required vs. provided:

- **Administrative Safeguards**
  - A covered entity must identify and analyze potential risks to e-PHI, implement security measures that reduce risks to a reasonable and appropriate level.
- **Technical Safeguards**
  - A covered entity must implement technical policies and procedures that audit, monitor, and allow only authorized persons to access e-PHI.
- **Physical Safeguards**
  - A covered entity must implement policy and procedures specifying proper use of the transfer, removal, disposal, and re-use of electronic media while limiting physical access to its facilities.
- **Policies, Procedures and Documentation Requirements**
  - A covered entity must adopt reasonable and appropriate policies and procedures and update/ review periodically in response to environmental and organizational changes to comply with the provisions of the security rule.
- **Organizational Requirements**
  - A covered entity that becomes aware of a business associate who has a material breach or violation of their contractual obligations must take reasonable steps to cure the breach or end the violation. The CE must update BA agreements requiring them to implement safeguards that appropriately protect e-PHI.

HIPAA Requirements – Administrative

HIPAA AREA	HIPAA REQUIRED	ASSESSMENT PROVIDED
Risk Analysis	✓	✓
Risk Management	✓	✓
Information System Activity Review	✓	✓
Assigned Security Responsibility	✓	✓
Workforce Security Authorization and/or Supervision		✓
Termination Procedures		✓
Information Access Management Isolating Healthcare Clearinghouse Function	✓	✓
Access Authorization		✓
Access Establishment and Modification		✓
Protection from Malicious Software		✓
Log-in Monitoring		✓
Password Management		✓
Security Incident Procedures Response and Reporting	✓	✓
Contingency Plan Data Backup Plan	✓	✓
Applications and Data Criticality Analysis		✓
Evaluation	✓	✓

HIPAA Requirements – Technical

HIPAA AREA	HIPAA REQUIRED	ASSESSMENT PROVIDED
Access Control Unique User Identification	✓	✓
Encryption and Decryption		✓
Audit Controls	✓	✓
Person or Entity Authentication	✓	✓
Transmission Security Integrity Controls		✓

HIPAA Requirements – Physical

AREA	REQUIRED	PROVIDED
Physical Risk Assessment	✓	✓
Appointing an Incident Response Officer (IRO)	✓	✓
Employee Training	✓	✓
Notification to Business Associates (BA)	✓	✓

HIPAA Requirements – Policy, Procedure, and Documentation

AREA	REQUIRED	PROVIDED
HIPAA Privacy & Security	✓	✓
HIPAA Breach Notification	✓	✓
IT Security	✓	✓
Document Destruction and Retention	✓	✓
Non-Pubic Information (NPI)		✓
Red Flags Amendment		✓
Social Media		✓
Portable Electronic Device		✓
Patient Privacy Notice	✓	✓
B.A. Agreement / Addendum	✓	✓

HIPAA Requirements – Organizational

AREA	REQUIRED	PROVIDED
Breach Response Plan	✓	✓
Corrective Measures Plan		✓
Notification/ update to Business Associates (BA)	✓	✓