

HIPAA Compliance

Contingency planning is a HIPAA Security standard. The objective of the contingency plan standard is to establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems containing electronic protected health information. ePolk's Offsite Backup Solution complies with all requirements of this standard by providing:

- ✓ User verification
- ✓ Role based authentication
- ✓ AES256 bit encryption of transmitted and stored data
- ✓ Offsite data storage in a remote location
- ✓ Hardened data storage facilities
- ✓ Informative reporting via email on status of backed up data

ePolk's Offsite Backup Solution is completely secure and can assure your organization that it can recover its data no matter what disaster it may incur. Please refer to the table below for a better understanding of how ePolk's Offsite Backup Solution enables businesses to instantly comply with HIPAA regulations:

HIPAA Privacy Rule	ePolk Offsite Backup	Covered Entity
Administrative §164.308		
§164.308(a)(2) Assigned Security Officer	YES	
§164.308(a)(4) Access Authorization	NO- Only covered entity has access to PHI	YES
§164.308(a)(6) Security Incident Reporting	YES	
§164.308(a)(7) Contingency Plan: Data Back-up	YES	YES
§164.308(a)(7) Contingency Plan: Disaster Rec.	YES	YES
§164.308(b)(1), 106.103 Business Associate Agreement	YES	...
Physical §164.310		
§164.310(a)(1) Facility Access Controls	YES	...
§164.310(d)(1) Device & Media Controls	YES	YES
Technical §164.312		
§164.312(a)(1) Access Control	YES	YES
§164.312(e)(1) Transmission Security	YES	YES
§164.312 Encryption of PHI	YES	YES
Other Security Standards		
§164.524 Access to PHI	NO – Covered Entity has the only encryption key	YES
§164.526 Amendment to PHI	NO – Covered Entity has the only encryption key	YES