

Item	Threat/Vulnerability	Remediation	Implemented Yes/No	Type of Safeguard	Likelihood	Impact	Risk	Included in Policies?
1	Unauthorized Access to Facilities, Network, and/or Disclosure, Loss, Destruction, Corruption, or Theft of ePHI							
1a	Disaster Recovery Plan is not in place	Implement a Disaster Recovery Plan(3)		Administrative	Medium	High	High	Disaster recovery policy
1b	Data Backup Procedures are not in place	Implement a Data Backup Procedure (4)		Administrative	Medium	High	High	Data Back up policy
1c	Hardware Redundancy is not in place	Ensure Hardware Redundancy is in place (5)		Administrative	Medium	High	High	Data Back up policy
1d	Lack of Employee Termination Procedures could allow a terminated employee to access data	Implement an Employee Termination Procedure to remove data access (8)		Administrative	Medium	High	High	Sanctions Policy
1e	Lack of Incident Response Procedure will leave organization unprepared for security breaches	Implement a Security Response Plan (9)		Administrative	Medium	High	High	HIPAA Security Management Policy
1f	Server room(s) not locked	Ensure all systems that contain ePHI are in a secure area (14)		Physical	Medium	High	High	
1g	Unrestricted access to server room(s) can lead to security breaches	Limit access to server room(s) (15)		Physical	Medium	High	High	
1h	Failure to track access to server room(s) can lead to security breaches	Limit entrance to and exit from the facility using one or more physical access methods. Secure keys, combinations, and other physical access devices. (16)		Physical	Medium	High	High	
1i	Unpatched systems can be exploited to gain access	Ensure systems have proper security patches applied at least quarterly (22)		Physical	Medium	High	High	
1j	Failure to track visitors and patients can lead to security breaches	Implement a procedure to track visitors and patients (25)		Physical	Medium	High	High	Facility Policy & Sign in sheet
1k	Password policy does not force complex passwords	Implement complex passwords; provide password set-up criteria to guide users in complex password set-up (26)		Technical	Medium	High	High	Password policy included but you need to ensure people are following the policy
1l	Password policy does not force password changes	Implement password aging/expiry (27)		Technical	Medium	High	High	Password policy included but you need to ensure people are following the policy
1m	Accounts are not disabled after failed password attempts	Disable user accounts after failed password attempts; establish maximum number of unsuccessful logins in order to determine when to lock the account (28)		Technical	Medium	High	High	Password policy included but you need to ensure people are following the policy