Security Service	HIPAA/HITECH Controls
Application Layer	
Web Application Firewall	Best practice- Implied under 164.306(A)
Network Layer	
Intrusion Detection	Best practice- Implied under 164.306(A)
Network Firewall (Hypervisor)	Best practice- Implied under 164.306(A)
External network vulnerability scanning	Best practice- Implied under 164.306(A)
Secure Remote Access (two-factor)	164.312(d), 164.312(a)(2)(iii)
Encryption in transit	164.312(e)(1)
Server Layer	
Hardened Operating System	Best Practice- Implied under 164.306(a)
Secure remote administrative access	164.312(d)
OS patching/updating	Best Practice- Implied under 164.306(A)
Anti-virus/anti-malware	164.308(a)(5)(ii)(B)
Log Management	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b)
Time Synchronization	Best Practice- Implied under 164.306(A)
File Integrity Monitoring	164.312(c)(2)
Physical layer	
Rogue wireless scanning	Best practice- Implied under 164.306(A)
Physical security	164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)(ii)
Administrative Controls	
Change control	Best Practice- Implied under 164.306(A)
Formal Risk Assessment	164.308(a)(1)
Incident Response	164.308(a)(6)
Data Backup	164.308(a)(7)(ii)(A), 164.310(d)(1), 164.310(d)(2)(iv)
Business Associate Contract	164.308(b)(1)
Maintain Maintenance Records	164.310(a)(2)(iv)
Access Control	164.312(a)(1)
Security Audits	164.308(a)(8)
Secure Data Deletion	164.310(d)(2)(ii)

The numbers in the right-hand column reference sections of the HIPAA/HITECH compliance standards.

Please visit HHS.Gov to learn more.