| | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 |  | | | | |
| 2 | **HIPAA Citation** | **HIPAA Security Rule Standard Implementation Specification** | **Implementation** | **Requirement Description** | **Solution** |
| 3 | 164.308(a)(1)(i) | *Security Management Process* | Required | Policies and procedures to manage security violations | |
| 4 | 164.308(a)(1)(ii)(A) | Risk Analysis | Required | Conduct vulerability assessment | Penetration test, vulnerability assessment |
| 5 | 164.308(a)(1)(ii)(B) | Risk Management | Required | Implement security measures to reduce risk of security breaches | SIM/SEM, patch management, vulnerability management, asset management, helpdesk |
| 6 | 164.308(a)(1)(ii)(C) | Sanction Policy | Required | Worker sanction for policies and procedures violations | Security policy document management |
| 7 | 164.308(a)(1)(ii)(D) | Information System Activity Review | Required | Procedures to review system activity | Log aggregation, log analysis, security event management, host IDS |
| 8 | 164.308(a)(2) | *Assigned Security Responsibility* | Required | Identify security official responsible for policies and procedures | |
| 9 | 164.308(a)(3)(i) | *Workforce Security* | Required | Implement policies and procedures to ensure appropriate PHI access | |
| 10 | 164.308(a)(3)(ii)(A) | Authorization and/or Supervision | Addressable | Authorization/supervision for PHI access | Mandatory, discretionary and role-based access control: ACL, native OS policy enforcement |
| 11 | 164.308(a)(3)(ii)(B) | Workforce Clearance Procedure | Addressable | Procedures to ensure appropriate PHI access | Background checks |
| 12 | 164.308(a)(3)(ii)(C) | Termination Procedures | Addressable | Procedures to terminate PHI access security policy document management | Single sign-on, identity management, access controls |
| 13 | 164.308(a)(4)(i) | *Information Access Management* | Required | Policies and procedures to authorize access to PHI | |
| 14 | 164.308(a)(4)(ii)(A) | Isolation Health Clearinghouse Functions | Required | Policies and procedures to separate PHI from other operations | Application proxy, firewall, mandatory UPN, SOCKS |
| 15 | 164.308(a)(4)(ii)(B) | Access Authorization | Addressable | Policies and procedures to authorize access to PHI | Mandatory, discretionary and role-based access control |
| 16 | 164.308(a)(4)(ii)(C) | Access Establishment and Modification | Addressable | Policies and procedures to grant access to PHI | Security policy document management |
| 17 | 164.308(a)(5)(i) | *Security Awareness Training* | Required | Training program for workers and managers | |
| 18 | 164.308(a)(5)(ii)(A) | Security Reminders | Addressable | Distribute periodic security updates | Sign-on screen, screen savers, monthly memos, e-mail, banners |
| 19 | 164.308(a)(5)(ii)(B) | Protection from Malicious Software | Addressable | Procedures to guard against malicious software host/network IPS, unified threat management, network anomaly detection, patch management, firmware management, host/network IDS, OS access controls (least-privileged user), content filtering | Network firewall, desktip firewall, antivirus, anti-spam |
| 20 | 164.308(a)(5)(ii)(C) | Log-in Monitoring | Addressable | Procedures and monitoring of log-in attempts host IDS | Log aggregation, log analysis, security event management |
| 21 | 164.308(a)(5)(ii)(D) | Password Management | Addressable | Procedures for password management | Password management software, single sign-on, metadirectories |
| 22 | 164.308(a)(6)(i) | *Security Incident Procedures* | Required | Policies and procedures to manage security incidents | |
| 23 | 164.308(a)(6)(ii) | Response and Reporting | Required | Mitigate and document security incidents | Helpdesk, vulnerability management, security event management |

| | A | B | C | D | E |
|---|---|---|---|---|---|
| 24 | 164.308(a)(7)(i) | *Contingency Plan* | Required | Emergency response policies and procedures | |
| 25 | 164.308(a)(7)(ii)(A) | Data Backup Plan | Required | Data backup planning and procedures | Backup support on-site/off-site |
| 26 | 164.308(a)(7)(ii)(B) | Disaster-Recovery Plan | Required | Data recovery planning and procedures | |
| 27 | 164.308(a)(7)(ii)(C) | Emergency Mode Operation Plan | Required | Business continuity procedures | |
| 28 | 164.308(a)(7)(ii)(D) | Testing and Revision Procedures | Addressable | Contingency-planning periodic testing procedures | |
| 29 | 164.308(a)(7)(ii)(E) | Applications and Data Criticality Analysis | Addressable | Prioritize data and system criticality for contingency planning | Change management control software, asset management software |
| 30 | 164.308(a)(8) | *Evaluation* | Required | Periodic security evaluation | Perform a periodic compliance assessment |
| 31 | 164.308(b)(1) | *Business Associate Contracts and Other Arrangements* | Required | CE implement BACs to ensure safeguards | |
| 32 | 164.308(b)(4) | Written Contract | Required | Implement coompliant BACs | Contracts |
| 33 | 164.310(a)(1) | *Facility Access Controls* | Required | Policies and procedures to limit access to systems and facilities | Policies and procedures |
| 34 | 164.310(a)(2)(i) | Contingency Operations | Addressable | Procedures to support emergency ooperations and recovery | Procedures |
| 35 | 164.310(a)(2)(ii) | *Facility Security Plan* | Addressable | Policies and procedures to safeguard equipment and facilities | Policies and procedures |
| 36 | 164.310(a)(2)(iii) | Access Control and Validation Procedures | Addressable | Facility access procedures for personnel | Card readers, locks, biometrics, proximity badges, tokens |
| 37 | 164.310(a)(2)(iv) | Maintenance Records | Addressable | Policies and procedures to document security-related repairs and modifications | Policies and procedures |
| 38 | 164.310(b) | *Workstation Use* | Required | Policies and procedures to specify workstation environment and use | Desktop management, policy management, application management |
| 39 | 164.310( c ) | *Workstation Security* | Required | Physical safeguards for workstation access | Card readers, locks, biometrics, tokens, hardware cables, proximity tokens, locking screen savers |
| 40 | 164.310(d)(1) | *Device and Media Controls* | Required | Policies and procedures to govern receipt and removal of hardware and media | |
| 41 | 164.310(d)(2)(i) | Disposal | Required | Policies and procedures to manage media and equipment disposal | Destruction, recycling |
| 42 | 164.310(d)(2)(ii) | Media Reuse | Required | Policies and procedures to remove PHI from media and equipment | Zeroing, degaussing |
| 43 | 164.310(d)(2)(iii) | Accountability | Addressable | Document hardware and media movement | Logs, receipts, cameras |
| 44 | 164.310(d)(2)(iv) | Data Backup and Storage | Addressable | Backup PHI before moving equipment | Tape/network backup, encrypted backup |
| 45 | 164.312(a)(1) | *Access Control* | Required | Technical (administrative) policies and procedures to manage PHI access | Policies and procedures |
| 46 | 164.312(a)(2)(i) | Unique User Identification | Required | Assign unique IDs to support tracking | Directories, OS user directories, ERP software, ID management software, single sign-on, metadirectories |
| 47 | 164.312(a)(2)(ii) | Emergency Access Procedure | Required | Procedures to support emergency access | Procedures |
| 48 | 164.312(a)(2)(iii) | Automatic Logoff | Addressable | Session termination mechanisms | Time-outs, proximity tokens, scheduled access control |
| 49 | 164.312(a)(2)(iv) | Encryption and Decryption | Addressable | Mechanism for encryption of stored PHI | File and folder encryption, hard drive encryption, e-mail encryption |
| 50 | 164.312(b) | *Audit Controls* | Required | Procedures and mechanisms for monitoring system activity | Log aggregation, log analysis, security event management, host IDS |
| 51 | 164.312( c)(1) | *Integrity* | Required | Policies and procedures to safeguard PHI unauthorized alteration | Policies and procedures |

| | A | B | C | D | E |
|---|---|---|---|---|---|
| 52 | 164.312( c)(2) | Mechanism to Authenticate Electronic Protected Health Information | Addressable | Mechanisms to corroborate PHI is not altered | PKI, digital signatures, OS/database/file hashing |
| 53 | 164.312(d) | *Person or Entity Authentication* | Required | Procedures to verify identities | SAML, PKI, ID management software, single sign-on, metadirectoreis, passwords, authentication tokens, digital certificates, biometrics |
| 54 | 164.312(e)(1) | *Transmission Security* | Required | Measures to guard against unauthorized access to transmitted PHI | Controls |
| 55 | 164.312(e)(2)(i) | Integrity Controls | Addressable | Measures to ensure integrity of PHI on transmission | Ipsec, VPN, S/MIME, PGP |
| 56 | 164.312(e)(2)(ii) | Encryption | Addressable | Mechanism for encryption of transmitted PHI | Ipsec, VPN, PPTP VPN, SSL VPN, S/MIME, SSH, PGP |