SCALEMATRIX
Cloud. Colocation. Managed IT.

HIPAA Matrix 2017

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) as found in 45CFR Part 106 and Part 164, Subparts A and E requires security standards be implemented in order to protect the confidentiality of personal health information (PHI). This is a requirement for Covered Health Care providers, Health Plans, Health Care Clearinghouses, and Medicare Prescription Drug Card Sponsors. In practical terms, and in light of ombudsman guidelines, this applies as well to any agency providing services in support of such providers, whether a Business Associate agreement is in place or not.

Approach

ScaleMatrix approaches these requirements through a strategy of transparency, and by constructing a matrix of controls to show proper mapping of the controls between the ScaleMatrix systems and the requirements. This allows any gaps in the controls to be identified and filled in properly by the client / second party, ensuring full compliance to the standards. Note that unless the environment is fully managed by ScaleMatrix there will always be controls gaps in ScaleMatrix' implementation.   In shared management cases, the minimum commitment from ScaleMatrix is that all solutions are compliant as originally delivered. ScaleMatrix is not in control of changes made after delivery to the client.

Requirements

The requirements are recognized as three broad categories: Administrative, Physical, and Technical. Each of these is covered below.

Administrative

Security Management Process (section 164.308)

Risk Analysis

ScaleMatrix conducts regularly scheduled meetings to discuss and analyze risks to the infrastructure and internal systems which support or host HIPAA data / systems. Corrective action is taken as soon as abnormal or unacceptable risks are identified to mitigate or remediate those risks.

Risk Management

Risk management is a basic design consideration for all systems. Specifically, factors such as failure patterns, attack area exposure, encryption, and siloing are core considerations for all solutions deployed.

Sanction Policy

Failure to comply with policies and procedures associated with data handling will result in sanctions up to and including termination. Policies are in place to enforce this.

Information System Activity Review

Logging is in place and centrally located. Logs have various scripted trips / alerts set into them to allow real time alerting and are reviewed at regular intervals for exceptions and issues.

Assigned Security Responsibility (section 164.308)

Security responsibilities are assigned clearly via policy.

Workforce Security (section 164.308)

Authorization

Separation of duties is strictly and technically enforced, with access being implemented on a minimum need to know basis. Authorizations are controlled via interface to a set of Active Directory structures.

Workforce Clearance Procedures

Managed as part of the inprocessing procedures with permissions assigned by current role. As responsibilities change, access controls are adjusted to allow or remove permissions appropriately.

Termination Procedures

Access is removed immediately from terminated personnel. Systems which are retired are logically disconnected from the network and the resources then reaped as soon as possible.

Information Access Management (section 164.308)

Isolating Health Care Clearinghouse Functions

All HIPAA environments are isolated from other environments via independent routed connections with separate firewalls for each environment. As delivered, all systems are fully isolated and accessible via secured protocols only.

Access Authorization

Authorization systems are controlled using group memberships and role-based access controls enforced technically. Group passwords / accounts are not implemented, allowing the principle of Non-Repudiation to be enforced properly.

Access Establishment and Modification

Covered thoroughly by policies and procedures covering hiring and job changes as well as periodic reviews of access systems for current access / permitted lists.

Security Awareness and Training (section 164.308)

Security Reminders

Reminders are handed out on a regular schedule and documentation of who has been informed per reminder, are retained.

Malware protections

Anti-malware programs (technical and procedural) on internal are in place, and exceptions are pursued to a defined conclusion. Impacting events caused by malware are tracked through the Incident Reporting system. Client deployments are free of malware as delivered and anti-malware programming is available through vShield if desired.

Log-in Monitoring / Logging

All access events are logged for infrastructure and ScaleMatrix internal systems. All access to client environments from the Orchestration, Virtualization, or Physical systems are fully documented.

Password Management

Strong controls are in place procedurally and technically for password issuance and maintenance.

Security Incident Procedures (section 164.308)

Response and Reporting

All variations from established configuration standards are treated as actionable and tracked in tickets or as Incidents. All variations which can be tracked to security violations are submitted for messaging to clients as well as opened as Incidents within internal systems. All client vulnerabilities which are discovered (ex. Heartbleed) are messaged and then scanned for, with repeated messaging until the vulnerability is closed.

Contingency Planning (section 164.308)

Data Backup Plan

ScaleMatrix maintains backups of all configurations and critical business data for internal purposes. Additionally, initial configuration data is backed up for clients. Client data is backed up as an added service. Snapshotting is available for clients within the public cloud at no expense, and all systems are designed to make client driven backups as convenient as possible.

Disaster Recovery Plan

Disaster Recovery / Business Continuity is a core competency for ScaleMatrix. The company has a DR plan in place to continue operations should there be a major fault at any single physical or logical location. All systems are deployed into either a fully meshed structure or completely compartmentalized structure to enable as efficient as possible recovery.

Emergency Mode Operation Plan (BC)

Emergency mode operations are covered by the ScaleMatrix DR/BC plan. Senior management at ScaleMatrix has had a great deal of experience running damaged or degraded systems with other companies, and with the challenges which ensue during such operations. All identified threats have been mitigated or remediated to the reasonable extent possible.

Testing and Revision Procedures

DR/BC plans are reviewed annually, and components of the plan are tested on a frequent basis.

Applications and Data Criticality Analysis

Applications, Data, and Infrastructure service are stack-ranked in order of importance and criticality, and protection of, or restoration of services is prioritized based on that ranking. External scanning of assets is performed monthly.

Evaluation (section 164.308)

Business Associate Contracts or Other Contractual Arrangements (section 164.308)

All business associates are identified by ScaleMatrix via use of a Business Associate Agreement. All agreements involving ScaleMatrix where ScaleMatrix is performing as the business associate are documented both in the internal control panel and via contract.

Physical

Physical Access Controls (section 164.310)

Contingency Operations

Contingency plans are in place to permit access and restoration of physical access control services in the event of an Incident.

Facility Security Plan

The facilities are protected in several ways, including armed security, extensive camera surveillance, biometric access controls at all entrances, and on each individual rack of equipment. Two factor authentication is required for client or employee access to the facility. Vendors are not permitted unauthorized access under any conditions.

Access Control and Authentication Procedures

No visitors are permitted without an escort and authorization. No undocumented visitors are permitted at all. Procedures are in place to validate visitors and ensure they are properly escorted. Note that visitors are not enrolled into the security system, thus have no access to anything other than the conference rooms and the bathrooms.

Maintenance Records

Comprehensive records are maintained for all maintenance and work performed on both the physical and logical equipment / configurations. All alterations to the ScaleMatrix systems are required to be processed through the Change Advisory Board.

Workstation Use (section 164.310)

Workstations are segmented by role and responsibility both logically and physically. Distance access is protected through the use of encryption and jump servers.

Workstation Security (section 164.310)

Workstations which are used in the configuration of EPHI systems are kept physically and logically secured, with two factor authentication required for physical access to the systems.

Device and Media Controls (section 164.310)

Disposal

Disposal of media is covered by policy requiring two person witnessed shred of the materials after they have been overwritten with random characters and then erased five times in succession. Should the media not be capable of being overwritten (i.e. it is physically damaged) it is shredded without being overwritten.

Media reuse

Media may be reused after being wiped and rewritten randomly five times in sequence.

Accountability

All materials capable of holding EPHI are tracked and accounted for. Ownership for all such materials is assigned.

Data Backup and Storage

All ScaleMatrix materials are backed up and the backups stored and maintained against failure or incident. Client systems may be backed up as a service.

Technical

Access Controls (section 164.312)

Unique User Identification

All users are uniquely identified. Group accounts are not allowed. All vendor default accounts are changed prior to provisioning of materials. All access to environments may be tracked through the unique identifier.

Emergency Access Procedure

Systems have been established to allow for secure emergency access assuming severely degraded systems and infrastructure. Jump servers, as well as iDrac and Avocent controls, are in place to assist in the event of a significant issue.

Automatic Session Termination

Session access is terminated automatically on a timer. All sessions are scanned during termination events and all outstanding sessions terminated immediately. VPN sessions are terminated automatically after a given time.

Encryption Management

All authoritative communications with clients is directed to the SSL protected ScalePortal. All communications into and out of the systems of ScaleMatrix are protected via SSL or AES (or better) encryption standards. Standards are checked quarterly for updates, and to ensure there are no known compromises / degradation of function. Note that client-maintained EPHI cannot be covered by ScaleMatrix encryption unless ScaleMatrix has logical access to the materials.

Audit Controls (section 164.312)

ScaleMatrix controls and systems are audited, both internally, and by two trusted third party elements, one for procedures and one for technical security controls.

Integrity (Data) (section 164.312)

ScaleMatrix offers File Integrity Management as a service to provide full integrity of data checking.

Person or Entity Authentication (section 164.312)

Authentication of all ScaleMatrix access events is implemented and monitored.

Transmission Security (section 164.312)

Integrity

All client environments are logically segmented from one another via individually routed and firewalled connections. Systems where clients “share a wire” are kept secure either through encryption protocols, vlan implementation with validation or segment assignments with validation.

Encryption

On ScaleMatrix managed solutions, encryption of data at rest is implemented to prevent alteration or exposure of the data. This also serves to validate integrity of the data when it is transferred from a backup status.