Data Privacy Governance Program

US HIPAA

zanda

APRIL 24, 2023

Policies and Procedures

Information security policies (summary info)

Access Control

Access Control Policy defines high-level requirements and guidelines on user account management, access enforcement and monitoring, separation of duties, and remote access.

Backup and Restoration

The organisation actively manages risks associated with data loss by defining a sound backup regime for all the data services.

Business Associate Template

This document guides the list of templates/forms from the "Guidance/Templates" section of Tugboat Logic Platform that are applicable to Business Associates.

Business Continuity and Disaster Recovery

The organisation has a Business Continuity and Disaster Recovery Policy that ensures that the organisation can quickly recover from natural and man-made disasters while continuing to support customers and other stakeholders.

Corporate Ethics

The organisation values ethics, trust and integrity throughout its business practices.

Data Retention and Disposal

This policy is about the organisation's approach for data retention and secure disposal.

Disciplinary Policy

The organisation has implemented a disciplinary process in order to deal with instance(s) of indiscipline including (but not limited to) non-compliance to information security policies and procedures by users.

Guidelines on Uses and Disclosure of Protected Health Information (PHI)

Guidance related to the appropriate uses and disclosures of Protected Health Information (PHI).

HIPAA Breach Notification Policy

Breach notification guidance for the organisation when impermissible or unauthorised access, acquisition, use, and/or disclosure of Individual's Protected Health Information (PHI) occurs.

HIPAA Internal Privacy Policy

Compliance with the administrative safeguards of HIPAA privacy rule, to secure and maintain the confidentiality of Protected Health Information (PHI).

Incident Management

It is critical to the organisation that security incidents that threaten the security or confidentiality of information assets are properly identified, contained, investigated, and remediated.

Information Security

Zanda utilises InfoSec Platform to manage policies, provide security awareness training, implement and document security controls, and track compliance with customers, third-party vendors, independent auditors and regulatory agencies.

Internal Audit

The organisation conducts Internal Audits on its existing policies and controls to ensure the best level of service to its customers.

Key Management and Cryptography

This policy aims to establish requirements for selecting cryptographic keys, managing keys, assigning key strengths and using and managing digital certificates.

Network Security

The organisation has a process to determine a person who lawfully qualifies as an individual's personal representative.

Personnel Security

Organisation members understand their roles and responsibilities around security and privacy.

PHI De-identification Policy and Procedure

Guidance related to the use and disclosure of de-identified information and how to de-identify protected health information (PHI).

Risk Assessment

The organisation institutes regular risk assessments and uses industry best practices in remediation.

Server Security

The organisation manages, configures and protects organisation servers and hosts based on industry best practices.

Vendor Management

The organisation actively manages risks around third-party vendors and their access to the organisation's data.

Vulnerability and Penetration Testing Management

The organisation conducts scheduled application and network scanning and penetration tests.

Workstation and Mobile Device

The organisation protects laptops and workstations and their contents using industry best practices.

Policy Implementation Controls

Breach

HB—Breach Assessments (R)

Risk Assessment is performed on the identified incidents following the discovery of a breach to determine the probability that PHI has been compromised and whether notifications are required.

HB—Breach Notification by Business Associates (R)

Roles and responsibilities of business associates with respect to breach notification is communicated as part of contractual obligations requiring them to notify data breaches, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except in cases stated by law enforcement official to delay the notification.

HB—Breach Notification to Authorities (R)

Procedures are in place to notify data breaches to appropriate authorities and media outlets. Such notifications are provided within 60 calendar days after discovery of a breach (if a breach affects 500 or more individuals) and no later than 60 days after the end of the calendar year (if a breach affects fewer than 500 individuals), except in cases stated by law enforcement official to delay the notification.

HB—Breach Notification to Individuals (R)

Notifications regarding breach of protected health information are provided to individuals impacted by the breach without unreasonable delay and no later than 60 days after discovering a breach.

HB—Methods of Notification (R)

The organisation has established a formal procedure on breach notification methods for notifying an individual, an individual's next of kin, or a personal representative.

Privacy

HP—Contract Terminations with Business Associates (R)

Upon termination of contract, the business associates/vendors are required to return or provide evidence of the destruction of protected health information in accordance with the contractual agreement.

HP—Notice of Privacy Practices (R)

Notice of organisation's privacy practices on uses and disclosures of PHI and individuals rights are provided to individuals whenever significant changes are made and at least once every three years.

HP—PHI of Deceased Individuals (R)

The organisation has developed a process to retain the PHI of deceased individuals for a period of 50 years following their death.

HP—Restriction on Uses and Disclosure of PHI (R)

Restriction on uses or disclosures of PHI requested by individuals is recorded, monitored and adhered to except when emergency treatment is required for the individual.

HP—Retention of Authorisations (R)

Formal data retention and disposal procedures are in place to guide the secure retention and disposal of PHI. Documentation, as required by HIPAA regulation, are maintained and retained for at least six years from the date of its creation or the date when it was last in effect, whichever is later.

HP—Uses and Disclosure of PHI (R)

The organisation has established formal policies and procedures on permitted and prohibited collection, use and disclosure of PHI. These policies and procedures are approved by management and communicated to employees and contractors.

HP—Uses and Disclosure of PHI by Business Associate (R)

Permitted and required uses or disclosures of protected health information by a business associate is defined in the business associate agreement/contract and implemented accordingly.

HP—Uses and Disclosures for Research Purposes (R)

The organisation has procedures in place relating to the use and disclosure of PHI for research purposes. The organisation retains documentation of such disclosures.

HP—Verification Requirements (R)

The organisation has defined processes to verify the identity and authority of a person requesting access to PHI. Request for access to PHI is facilitated based on verification of documentation, statements, or representations and the identity of the person requesting such access.

Security

HS—Access Authorisation to ePHI (A)

Access to ePHI requires a documented access request and approval from designated management personnel prior to access provisioning.

HS—Business Associate Agreement (R)

Business associates or vendors working on behalf of the organisation and with access to PHI are required to sign an agreement outlining the security and privacy requirements for protecting PHI.

HS—Access Control Policy and Procedure (R)

The organisation has established and implemented an access control policy and procedure that governs access rules for granting access to ePHI and is reviewed by management annually.

HS—Access to Workstations (R)

Access to workstations that store or access ePHI is restricted to authorised users and provisioned based on the formal authorisation process.

HS—Antivirus Software (A)

Antivirus software is installed on systems containing ePHI to prevent or detect the introduction of unauthorised or malicious software, and it is configured to force updates when available.

HS—Assigning Security & Privacy Responsibilities (R)

Management has designated a security and privacy official to oversee the development and implementation of security and privacy policies and procedures.

HS—Backup Restoration (R)

Backup restoration testing is performed on a quarterly basis to test the integrity and completeness of back-up data. Incident Management Process is invoked for anomalies.

HS—Business Continuity Plan (R)

A business continuity plan (BCP) and Disaster Recovery Plan (DRP) have been developed and tested annually (including procedures on the protection of ePHI while operating in emergency mode). Test results are reviewed, and plans are updated, if required, based on the outcome of the test performed.

HS—Business Impact Analysis (A)

The organisation has established a formal Business Impact Analysis process to assess PHI applications' criticality and data to drive business continuity requirements.

HS—Data Backup and Monitoring (R)

Data backups are performed regularly in accordance with an approved backup policy. Backups are monitored for failure using an automated system, and appropriate corrective actions are taken.

HS—Data Backup and Restoration Procedure (R)

Formal procedures that outline the data backup and restoration process are documented. The procedures are reviewed by IT management annually or in case of significant changes.

HS—Data Disposal Policy (R)

Data disposal policy is in place to guide secure disposal of ePHI or media containing ePHI, including guidelines on media sanitisation before re-use.

HS—Disciplinary Process (R)

Organisation has established a formal disciplinary process describing actions to be taken against employees and contractors who fail to comply with the organisation's security and privacy policies and procedures. The formalised disciplinary process is communicated to and acknowledged by employees and contractors.

HS—Emergency Access Procedure (R)

Emergency Access procedure has been established to obtain electronic protected health information during an emergency.

HS—Encryption of Data at Rest (A)

Electronic Protected Health Information (ePHI) is encrypted at rest (stored and backup) using strong encryption technologies.

HS—Encryption of Data in Transit (A)

Encryption technologies are used to protect the communication and transmission of ePHI over public networks and between systems.

HS—Incident Management Process (R)

A formal incident management process has been established, which requires incidents (breaches) to be tracked, documented and resolved in a timely manner in accordance with the breach notification rule. The process document is reviewed and updated by management on an annual basis.

HS—Incident Resolution and Response (R)

Incidents related to security and privacy are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with the formal incident management process.

HS—Internal Control Assessment (A)

On a periodic basis, management reviews the effectiveness and efficiency of processes and safeguards implemented for PHI's security and privacy. Identified issues are followed up, and appropriate actions are taken in a timely manner.

HS—Key Management and Cryptographic Policy (A)

A policy on the use of cryptographic controls and key management for the protection of electronic information is developed and implemented.

HS—Log Management Process (A)

The organisation has established and implemented a formal log management procedure for monitoring log-in attempts and reporting discrepancies. Access to change log configurations or to modify logs is restricted.

HS—Logging and Monitoring (R)

Logging is enabled to record administrative activities, access login attempts and security events and monitored on a regular basis. Automated alerts are configured, notifying IT management of any security issues followed up and resolved in a timely manner through the incident management process.

HS—Maintenance and Retention of Records (R)

Records of assessments and activities required to be performed as per defined policies and procedures are maintained and retained for six years from the date of its creation or when it was last in effect, whichever is later.

HS—Media Handling Policy (R)

A media handling policy and procedure have been established and implemented that governs any media movement containing ePHI into or out of the facility.

HS—Network Diagram (R)

A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.

HS—Penetration Testing (R)

Penetration testing is performed on an annual basis on networks and applications. Issues identified are classified according to risk, analysed and remediated in a timely manner.

HS—Policies and Procedures (R)

Organisation has established security and privacy policies and procedures for protecting PHI, which is communicated to all employees and contractors. These policies and procedures are reviewed and approved by management on an annual basis or in case of significant changes.

HS—Review of Access to ePHI (A)

User access to information systems containing ePHI is reviewed by management quarterly to assess appropriateness. Corrective actions are documented and resolved in a timely manner.

HS—Revoke Access to ePHI (A)

User access to information systems containing ePHI is revoked in a timely manner upon employment or contract termination.

HS—Risk Assessment of ePHI (R)

Management performs a formal risk assessment to identify potential risks and vulnerabilities related to confidentiality, integrity, and availability of PHI (including electronic) on an annual basis or in the event of significant changes. Identified risks, along with mitigation strategies, are documented and implemented by the organisation's management.

HS—Security and Privacy Awareness Training (R)

Employees and contractors are required to complete an information security and privacy awareness training as part of the onboarding process and annually thereafter.

HS—Security Review of Business Associates (R)

On an annual basis, the organisation performs a review of business associates or vendors with access to ePHI to assess their compliance to agreed-upon security, confidentiality, and privacy requirements.

HS—Unique IDs and Strong Passwords (R)

Unique user IDs and strong passwords are required in order to gain access to systems containing ePHI.

HS—Vulnerability Scanning (R)

A vulnerability scan (external and internal) is performed on a quarterly basis to identify system vulnerabilities containing PHI. Issues identified are analysed and remediated in a timely manner.

HS—Workstation Security Policy (R)

Workstation security policy and the procedure have been established that specifies security measures to be implemented on workstations that store or access ePHI.