Base64.ai

HIPAA Report

June 13, 2022

Powered by 

Overview

Base64.ai provides data extraction AI services from all document types, meaning no more manual document entry. Base64.ai provides solutions for: COVID-19 & Vaccination Cards, Background Check, Gig Economy, Ride Sharing, Airlines, Logistics, Customer Onboarding, and much more. Additionally, Base64.ai offers five integration methods, to allow their AI to seamlessly integrate with your software: API Integration, No-code AI, On-premises, and using using their Platform Partner or Solution Partners.

Security and Risk Management

Base64.ai has a security steering committee with oversight over information security, risk assessment, risk management, and privacy. This committee exercises the overall function of enabling secure cyber practices within the organization. This includes a commitment to information assurance.

Cyber security and privacy policies, as well as standards, procedures, guidelines and other supporting documents, are established, maintained, and disseminated throughout the organization. All staff are trained on these documents upon hire and at least annually thereafter. Internal committees work to monitor the cyber and privacy landscapes, ensuring governance documents are reviewed and updated in a timely fashion, but no less than annually.

Base64.ai retains a risk register, which contains entries from the business impact assessment, supply chain risk assessment, data protection impact assessment and the company's overall risk assessment. Each entry is assigned an owner and is updated regularly among the risk/oversight committee.

Base64.ai has established partnerships with others in the information security and privacy arena enabling prompt responses to incidents to include partnership with law enforcement agencies.

Assigned Security Responsibility

Base64.ai has assigned individuals with responsibility over audit, risk assessments, and risk management. Specifically, an executive level member has been appointed the Security Official role responsible for the organization's adherence to HIPAA. This role is responsible for creating a strategy for compliance with HIPAA, performing an evaluation of the organization, documenting the results of the evaluation, and reevaluating the organization periodically.

Workforce Security

Upon hiring and annually thereafter, all employees must successfully complete training courses covering the HIPAA Security Rule, HIPAA Privacy Rule, and basic information security practices supporting the function of an effective risk management program. The training courses are designed to assist employees in identifying and responding to social engineering attacks

(phishing, pharming, and tailgating) and in avoiding inappropriate security practices (for example, writing down passwords or leaving sensitive material unattended).

Employee roles and responsibilities are defined, including those roles having access to or supervising others with access to protected health information (PHI). Before access to PHI is granted, the scope of PHI is reviewed to ensure it is appropriate.

If an employee is found to be violating company policies, additional training is provided, or other disciplinary actions are taken.

Employees with specific incident response responsibilities have additional requirements to complete incident response training once a year.

Information Access Management

Access management processes exist so Base64.ai's employee and contractor user accounts are added, modified, or disabled in a timely manner as well as reviewed on a quarterly basis. In addition, password configuration settings for user authentication to Base64.ai are managed in compliance with Base64.ai's Password Policy, which is part of the Information Security Policy.

Users must be approved for logical access by senior management prior to receiving access to Base64.ai. Management authorization is required before employment is offered and access is provided. Users must also be assigned a unique ID before being permitted access to system components. User IDs are authorized and implemented as part of the new hire onboarding process. Access rights and privileges are granted to user IDs based on the principle of least privilege and Role-Based Access Control (RBAC) protocols. Access is limited to only what is required for the performance of job duties for individual users. Generic access by Base64.ai's employees is prohibited.

Access reviews are performed semi-annually to ensure employees' access meets the definition of "minimum necessary" as outlined in the Access Control portion of the Information Security Policy. In the event of a departure from the organization, access to all systems is terminated within twenty-four (24) hours.

Security Awareness and Training

Base64.ai's employees, contractors, and other contingent staff are required to undergo security awareness training upon hiring, changing roles, and at least annually to include, where applicable: HIPAA; and/or secure engineering/coding practices.

Security Incident Response and Reporting

An Incident Response Policy and procedures manual has been formally documented and implemented to guide the organization through handling of different types of security breaches/incidents including: preparation; detection; response; analysis and repair;

communication; follow-up; training; and testing. The responsibilities in the event of a breach, the steps of a breach, and the importance of information security are defined for all employees. The Incident Response Team employs industry-standard diagnosis procedures (such as incident identification, registration and verification, as well as initial incident classification and prioritizing actions) to drive resolution during business-impacting events.

Base64.ai reviews, triages, and communicates all incident alerts whereupon the Incident Response Team starts the incident response process. Post-mortems are convened after any significant operational issue, regardless of external impact. Documentation of the investigation is conducted to capture the root cause and determine preventative actions to take in the future.

At the time of this assessment, Base64.ai has identified no significant security incidents having triggered the incident response process. Base64.ai has performed their annual incident response test.

Business Continuity and Disaster Recovery

Base64.ai is committed to maintaining its business operations, in the face of any event. Base64.ai has studied the various impacts to the business by completing a business impact analysis. This business impact analysis is documented and updated at least annually. After completing this exercise, the organization gathered stakeholders to create the business continuity (BC) and disaster recovery plan (DR). In the BC/DR plan, the organization discusses coordination of activities to provide continued services to customers.

Base64.ai has developed and implemented a comprehensive data backup as well as recovery process to ensure all sensitive/confidential data is backed up, retained, and recoverable based on services provided by their cloud hosting platform. Following a significant business disruption, the organization immediately assesses the extent to which the disruption corrupted or lost any critical data. Backups are scheduled to occur at least daily, and be retained for seven (7) days. If required, Base64.ai will immediately restore corrupted or lost data from the most recent backup, or restore services by migrating/deploying services to another region.

Technical Evaluations

Base64.ai performs an annual technical and nontechnical evaluation, based initially upon the standards implemented under the HIPAA Security Rule and subsequently, in response to environmental or operational changes impacting the security of sensitive/classified information establishing the extent the organization’s security policies/procedures meet regulatory requirements.

Third Party Risk Management

When choosing a new vendor, Base64.ai follows a standard due diligence process. Third-party providers are researched, interviewed, reviewed internally, and then selected. A statement of work is required to define the terms of service, timelines, and deliverables. Service level

agreements (SLAs) are recommended to define performance consistency, shared defined responsibilities, and system redundancy, if applicable. Once implemented, third-party service providers are monitored. Base64.ai requires third parties to sign a nondisclosure agreement (NDA) prior to sharing information with them.

In addition, contracts must also include clauses stipulating the Third-Party Vendor will comply with applicable contractual obligations, standards, laws, and regulations. Where sensitive and confidential information is shared, the contract must include clauses requiring data security responsibility and notification in the event of a breach. The Third-Party Vendor contract defines the types of information gathered by Base64.ai as well as the uses or disclosures for this information within the organization. This includes specifics on confidential information. All critical vendors are requested to provide a SOC 2 attestation or ISO certification at least annually. Base64.ai reviews this document (or materials substantially similar) at least annually to ensure third parties meet Base64.ai's Supplier Risk criteria.

Third parties who exchange PHI with Base64.ai are required to have Business Associate Agreements (BAA) in place, prior to any data exchange. These business associate agreements are reviewed periodically and include provisions to ensure the safe handling of PHI by the vendors. Such contracts include requirements to report security incidents to Base64.ai. These contracts, where PHI is exchanged, limit the use and disclosure of PHI to only what is permitted by the contract and all parties involved.

Physical Security and Environmental Controls

Physical controls are in place to protect against external and environmental hazards, such as fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters. The Base64.ai infrastructure is hosted by a cloud service provider, which is responsible for the hosted data's environmental security. All Base64.ai data is physically secured by the cloud service provider. The cloud service provider provides sufficient physical controls to protect sensitive data and Base64.ai regularly reviews the cloud service provider's audit reports to ensure security and compliance needs are met.

Workstation Use and Security

Base64.ai maintains a system of controls and requirements to prevent unauthorized access, modification, destruction, or disclosure of sensitive and confidential data. Base64.ai classifies its data by identifying the types of data being processed and stored as well as determining the sensitivity of the data along with the likely impact arising from a compromise, loss, or misuse of the data. Unless otherwise required by law, Base64.ai retains sensitive and confidential data only for as long as necessary to fulfill the purposes for which it is collected and processed or to meet legal and contractual obligations.

Furthermore, Base64.ai has enabled data loss protection on the document repository and e-mail system.

Base64.ai maintains an asset inventory. All sensitive or confidential data is encrypted both at rest and in transit.

Disposal

Policies/procedures are maintained to address disposal of PHI and/or the hardware/ electronic media on which it is stored. Procedures specify the use of technology/software to make PHI on hardware/electronic media unusable and inaccessible. All media containing ePHI is security wiped or physically destroyed when no longer used.

Access Controls

Base64.ai maintains an Access Control Policy defining role based access criteria. Access procedures include the utilizing of user access authorization forms evidencing approval of access. The Access Control policy details processes for adding, modifying, and deleting user access. This policy is approved and updated at least annually. Privilege access is restricted to a limited number of authorized users.

The organization maintains information systems having automatic logoffs.

Base64.ai's Information Security Policy defines the appropriate encryption standards, which is based on FIPS standards, NIST standards, and OWASP recommendations.

Audit Controls

Logs and system records from various elements of the operating environment are consolidated into a single source for ingestion by a log aggregation platform. This provides assurance to the organization's security posture in providing a baseline for operations, and aids in discovery of abnormal activity.

Documents containing PHI or relating to HIPAA must be maintained for at least six (6) years.

Integrity Controls

The organization implements adequate policies/procedures to secure PHI from improper alteration or destruction. The annual risk assessment ensures a review of the controls to protect the Integrity of PHI. Any abnormal behavior identified or unexpected access is handled through the Incident Response process.

Authentication

The organization's platform requires multi-factor authentication utilizing a password and authenticator application.

Transmission Security

Cryptographic controls are essential to the protection of Base64.ai data. All data in transit is encrypted with TLS 1.2 or above.

Documentation

Should you need specific documentation as it refers to the above topics, please contact Base64.ai customer support at https://base64.ai/contact.

About Laika

Laika helps businesses manage compliance, obtain security certifications, and build trust in the marketplace. With Laika's software platform powered by expert guidance, it has never been easier to implement, demonstrate, and maintain compliance. From control implementation to vendor management, workflows are centralized and automated while Laika's concierge team streamlines audit prep and management through enterprise procurement.

Learn more at www.heylaika.com.