intelligencebank dam

HIPAA Compliance Overview

intelligencebank.com/dam

make.work.seem.less

IntelligenceBank supports the HIPAA (Health Insurance Portability and Accountability Act) regulations, and is able to sign HIPAA Business Associate Agreements (BAA's) with enterprise-level customers as required. HIPAA is a US federal mandate that requires specific security and privacy protections for Protected Health Information (PHI).

Although there are no official government or industry certifications for HIPAA compliance, IntelligenceBank has reviewed the HIPAA regulations and has ensured our controls, policies and procedures adhere to requirements to be HIPAA compliant. Following is an overview of measures IntelligenceBank takes for HIPAA compliance around security, privacy, administration and notifications.

Following is how IntelligenceBank complies with HIPAA security regulations:

1. **Unique User Identification** - Users that Customer Admins put into the IntelligenceBank platform are uniquely identifiable and are assigned a unique username and password for tracking.
2. **Emergency Procedures -** There is an established procedure to identify and extract ePHI during an emergency.
3. **Automatic Logoff** - Within the Admin tab of the IntelligenceBank system, Customer Admins can determine procedures that terminate a session after a specified time of inactivity.
4. **Encryption -** All data stored within IntelligenceBank is encrypted at rest and in transit.
5. **Audit Controls** - Implemented hardware, software, and technical processes that record and examine activity in information systems that contain or use ePHI are audited. Specifically, IntelligenceBank's technical controls are audited externally through an annual SOC 2 audit and IntelligenceBank adheres to ISO27001 controls. IntelligenceBank's premium data center is also SOC 1 and 2 compliant and ISO27001 certified.
6. **Authenticate ePHI** - Electronic systems are in place to verify that ePHI has not been altered or destroyed inadvertently.
7. **Authentication** - Customer Admins will Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
8. **Transmission Security** - ePHI records transmitted are not modified without tracking until properly removed from the system.
9. **Contingency Operations** – Within IntelligenceBank's established and tested disaster recovery plan, there is access to ePHI to support restoration of data in case of loss or tampering during an emergency.
10. **Facility Access Controls** - IntelligenceBank's data centre, AWS has a suite of best practice physical and environmental controls, including access control validation and maintenance records to secure ePHI. The AWS whitepaper can be accessed here: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
11. **Workstations –** IntelligenceBank's workstation policies state and specify how workstations that access ePHI should be configured, how access should be performed and various physical attributes of the workstation environment. This includes physical workstation security.
12. **Media Disposal** – IntelligenceBank adheres to customer requirements for sanitizing servers and disposing of ePHI data upon termination. In addition, ePHI is removed from electronic media if re-used, such as a hard drive and records are kept with regards to the movements of hardware and persons in control responsible.
13. **Data Backups -** IntelligenceBank has extensive backup processes – one time on site and another time off site. As such, we are able to retrieve an exact copy of ePHI when required as per the latest version stored within IntelligenceBank.

There are also a range of Administrative measures IntelligenceBank employs that include policies, procedures and contractual arrangements that govern IntelligenceBank staff and how they relate to security measures to protect ePHI.

1. **Risk Analysis and Management** – IntelligenceBank maintains a risk register which includes how ePHI records hosted on behalf of customers are being used and stored to ensure there is no violation with HIPAA compliance. Each risk has a rating and associated control, policy, review and ramifications if an employee does not abide by protocols.
2. **Information Systems Activity Reviews** – On a regular basis, IntelligenceBank reviews all logs, system activities (required): Regularly review system activity, logs, audit trails, etc.
3. **Assigned Security Officers** – IntelligenceBank has designated IS security officers who are responsible for all compliance frameworks including ISO27001, HIPAA and SOC 2.
4. **Employee Access Limits** – An employee's access to ePHI ends when his or her tenure with IntelligenceBank is terminated. Partner organizations and sub-contractors are not permitted to access ePHI records.
5. **Information Access Management** – IntelligenceBank has procedures for granting access to any sensitive information, including ePHI and there are formalized systems to grant access if necessary.
6. **Security Awareness and Training** – Upon induction and on an annual basis, IntelligeneBank conducts security and awareness training to new and existing employees. eLearning quizzes are administered annually to ensure staff understand all security and privacy policies, and procedures. This includes procedures on guarding against, detecting and reporting malware. IntelligenceBank also includes procedures for creating, changing, and protecting passwords.
7. **Login Monitoring** - Institute monitoring of logins to systems and reporting of discrepancies.
8. **Incident Reporting** – IntelligenceBank has a system and process to identify, document, and respond to security incidents.
9. **Contingency Plans** – IntelligenceBank has full, periodically tested, accessible backups of ePHI and there are documented procedures to restore data. This includes business continuity plans to enable continuation of critical business processes and protection of data in case of an emergency.
10. **Evaluations** – IntelligenceBank regularly performs assessments to see if any changes in the law require changes to HIPAA compliance procedures.
11. **Business Associate Agreements** - IntelligenceBank signs BAA (Business Associate Agreement) addendums with its enterprise level customers who need to be HIPAA compliant. The signed BAA will be established prior to Protected Health Information (PHI) being uploaded to IntelligenceBank.
12. **Breach Notification** – Should a data breach occur involving ePHI, IntelligenceBank, will promptly notify customer administrators who have an obligation to notify the affected parties if the breach affects more than 500 individuals.

Last but not least, the HIPAA Privacy Rule requires appropriate policies, systems and controls to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients-rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. Here are the controls IntelligenceBank has in place to adhere to the HIPAA privacy compliance:

1. Do not allow any impermissible uses or disclosures of PHI.
2. Provide breach notification to the Client who then will advise the person involved.
3. Provide either the individual or the Covered Entity access to PHI.
4. Disclose PHI to the Secretary of HHS, if required to do so.
5. Provide a full summary of disclosures.

For additional information, please contact compliance@intelligencebank.com.