# Kintone HIPAA Compliance White Paper

Kintone Corporation & Cybozu, Inc.

October 2025

## About this White Paper

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. law established as a standard to protect the confidentiality, integrity, availability, and security of Protected Health Information (PHI). With the increasing digitization of healthcare, there is growing recognition of the importance of protecting electronically Protected Health Information (ePHI). Kintone Corporation provides services that meet HIPAA standards in order to support our customers' HIPAA compliance.

This white paper describes the status of Cybozu, Inc. (“Cybozu” below) compliance with the requirements of the HIPAA Security Rule for the development and operation of the cloud service Kintone, which is provided by Kintone Corporation.

## Main Security Initiatives at Cybozu

At Cybozu, various initiatives are implemented to ensure the security of Kintone. Some of the notable features are as follows:

1). Availability and reliability

Kintone utilizes the hosting infrastructure of Amazon Web Services ("AWS" below) and adopts a geographically redundant replication configuration in multiple availability zones,* achieving high availability and reliability. In addition, our commitment to security with customers is clearly stated in the "Service Level Objective (SLO)" and is published on the Kintone Corporation website.

* We utilize Amazon RDS Multi-AZ service.
  For details regarding availability, please refer to the AWS site (https://aws.amazon.com/rds/features/multi-az/).

2). Access control and encryption of stored data

Kintone provides various access control features, including authentication via account and password, SSO authentication using Security Assertion Markup Language (SAML), and, if necessary, multi-factor authentication (IP address restrictions, code issuance via authentication apps), as well as lockout settings for authentication failures. Additionally, customer data stored in Kintone is encrypted using AWS features (such as AWS RDS, S3), and all communications between the server and web browser are encrypted.

3). Established the Cy-SIRT* team dedicated to security incident response

Cybozu has established a specialized team called Cy-SIRT to respond to various security incidents both inside and outside the

company. Cybozu's CSIRT organization (Cy-SIRT) also works with outside organizations and experts to prevent incidents, detect them early, resolve them promptly, and minimize damage should any occur. Our goal is to provide products and services that customers can use with peace of mind.

4). Security audits by third-party organizations

Cybozu has built a process to evaluate and improve overall security measures in accordance with the Plan-Do-Check-Act (PDCA) cycle, and all risks and mitigation measures are managed under the responsibility of the Information Security Management Officer. As objective proof of this, security audits are conducted by various third-party organizations.

The contents described in this white paper are primarily based on Cybozu's Information Security Management System (ISMS) and Kintone's SOC2 Type II Report.

▼ Main security audits by third-party organizations

- ISO/IEC 27001 (Information Security) Certification ("ISMS Certification" below)

  Cybozu obtained ISMS certification for its Information Security Management System (ISMS) in 2011 and has maintained it ever since.

  □ Certification scope:
    - Design, construction, and maintenance of operational infrastructure for our in-house developed cloud services
    - Design, construction, operation and maintenance of our internal information system infrastructure
    - Development of cloud services, on-premises products, and internal systems

  □ Certification number: IS 577142

- Received SOC 2 Type II Assurance Report

  Cybozu has received a System and Organization Controls (SOC) 2 Type II Assurance Report on internal controls for the Kintone service.

  If you require a Kintone SOC 2 Type II Report, please visit the Kintone Trust Center (https://trust-center.kintone.com/).

- TX-RAMP (https://dir.texas.gov/resource-library-item/tx-ramp-certified-cloud-products)
- Other regular vulnerability audits and penetration testing audits

## Kintone Compliance Status in Each of the HIPAA Categories

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| **Administrative Safeguards** | | | |
| §164.308 (a)(1) | Security Management Process | Implement policies and procedures to prevent, detect, contain, and correct security violations. | At Cybozu, under supervision of the Information Security Management Officer, we analyze threats and potential risks to the provision of Kintone services and potential business impacts, based on which we formulate response plans and implement measures aimed at avoiding or reducing those risks. Additionally, we regularly undergo external audits by third-party organizations, and appropriate measures are taken when risks are identified.<br>Cybozu has established policies, manuals, annual plans, etc., regarding information security management, and we develop and operate Kintone based on these. As part of the information security management PDCA cycle, internal audits are conducted, as are periodic checks to ensure that the management cycle, including the review process, is being conducted appropriately, and corrective actions are being taken on points that require improvement.<br>In relation to security in Kintone, measures are implemented from the perspectives of confidentiality, integrity, and availability. To ensure confidentiality, measures implemented against unauthorized access and unauthorized logins to Kintone include: providing features such as client authentication, SAML authentication, two-factor authentication, access source IP address restrictions, protecting login accounts, and obtaining audit logs. To ensure integrity, backups of the data stored in Kintone are performed. To ensure availability, Kintone utilizes AWS's hosting |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | | infrastructure, adopting a geographically redundant replication configuration across multiple availability zones to achieve high availability and reliability. |
| § 164.308 (a)(2) | Assigned Security Responsibility | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity or business associate. | At Cybozu, we have established and operate a team structure in which, under the Information Security Management Officer, the specialized team tasked with dealing with security incidents Cy-SIRT and a cross-company meeting body specializing in security, the Cybozu Security Meeting (CSM), collaborate to maintain and enhance security from a technical, operational, and control perspective.<br>In the construction of Cybozu's ISMS, it is clearly stipulated that goal setting, approval, and management reviews are to be conducted. Under the direction of management and the Information Security Management Officer, risk analysis is performed annually, and the results are continuously processed for management review, thereby systematically implementing the maintenance and improvement of security measures. |
| § 164.308 (a)(3) | Workforce Security | Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | In relation to employee security, the necessary information security competencies and knowledge required are defined for each position. Additionally, for information owners and personnel engaged in operations that fall within the scope of the ISMS, their roles are correctly communicated to them, and training is conducted. When hiring employees, a profile of the ideal candidate is defined from an information security perspective, and interviews and hiring activities are conducted accordingly.<br>When an employee resigns or their contract ends, access rights to the assets and systems granted to them are returned or revoked based on |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | | a process with defined procedures. A list of the items loaned to the employee that are to be collected back from them and a process for changing access rights during employee leave of absence, or when they resign, have also been established to prevent any inappropriate accounts, access rights, or authentication devices remaining. |
| § 164.308 (a)(4) | Information Access Management | Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. | Cybozu has established a strict access management system to protect customer data. The database that stores customer data is located in an area that cannot be directly accessed from the internet, and appropriate access rights are set.<br>Employees who operate and maintain Kintone access the Management Console (AWS Management Console) on which administrator work is done using a separate Operation Terminal from the devices used for routine operations. Operations in the service environment are conducted via the Management Console through the Bastion (jump server). When employees who perform operations and maintenance access the Management Console, appropriate access rights are set for each employee through Single Sign-On (SSO) integration with the company-wide authentication infrastructure.<br>Additionally, as part of the PDCA cycle, regular access rights inventories are taken and reviews of access rights granting criteria conducted. |
| § 164.308 (a)(5) | Security Awareness and Training | Implement a security awareness and training program for all members of its workforce (including management). | In relation to training and raising employee security awareness, training needs are defined based on the necessary competencies and qualifications predetermined for each job role, based on which an annual information security education plan is developed. Furthermore, after training is conducted its effectiveness is measured, and feedback is |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | | incorporated into the content of the training course for the following year, thereby achieving continuous improvement. Moreover, rigorous specialized security training is conducted, including secure coding training delivered through external seminars, etc.<br>Specifically, in addition to the security training delivered upon joining, all employees engaged in development and operations are required to take annual security training and pass a test on their understanding of the content of the training. Additionally, employee completion of these training sessions is monitored, and a system is in place to enable appropriate follow-up based on the employee's understanding level. |
| § 164.308 (a)(6) | Security Incident Procedures | Implement policies and procedures to address security incidents. | In relation to the response to security incidents, Cybozu has established a "definition of information security incidents" and defined roles and responsibilities for incident response in accordance with the "incident response process" based on the level of the incident. In addition, we have established the Cybozu Computer Security Incident Response Team (Cy-SIRT) as the CSIRT organization to respond to incidents. Cy-SIRT consists of members from the Cybozu Product Security Incident Response Team (Cy-PSIRT), which includes security engineers from the Security Office and the development divisions.<br>When an incident occurs, the details of the incident, response, and measures to prevent reoccurrence are centrally recorded and managed in the Incident Management App, and reported to the information owner, as well as escalated to management based on the level of the incident. |
| § 164.308 (a)(7) | Contingency Plan | Establish (and implement as needed) policies and procedures for responding to an emergency or | In relation to emergency response, Cybozu has developed a Business Continuity Plan (BCP) aimed at ensuring the continuous provision of |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | services or quick recovery, along with technical and physical measures, in the event of a significant system failure. Additionally, we conduct BCP training at least once a year to verify the effectiveness of the BCP. |
| § 164.308 (a)(8) | Evaluation | Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart. | At Cybozu, as part of the effectiveness verification in ISMS, processes, responsibilities, and implementation matters related to the performance evaluation of security management measures are defined, and evaluations based on these definitions are performed periodically. We also conduct internal audits regarding compliance with HIPAA Security Rule requirements, vulnerability assessments, penetration testing audits, and other external audits are conducted by third-party organizations at least once a year.<br>In the construction of Cybozu's ISMS, it is clearly stipulated that goal setting, approval, and management reviews are to be conducted. Under the direction of management and the Information Security Management Officer, risk analysis is performed annually, and the results are continuously processed for management review, thereby systematically implementing the maintenance and improvement of security measures. |
| § 164.308 (b)(1) | Business Associate Contracts and Other Arrangements | A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will | AWS is considered a critical subcontractor in the development and operation of Kintone. Cybozu has entered into a Business Associate Agreement (BAA) with AWS, and regularly checks the HIPAA compliance of the AWS services it uses and the details of AWS's security measures. |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | appropriately safeguard the information. | |
| **Physical Safeguards** | | | |
| § 164.310 (a) | Facility Access Controls | Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | Since the internal controls related to physical access to the Kintone system are maintained by AWS, they are excluded from the evaluation.<br>Access to the service environment where the Kintone system is installed is controlled so that only a dedicated operational terminal, separate from the terminals used for routine operations, can access it. Surveillance cameras are installed in the workspace area to control access, etc.<br>An emergency action plan has been formulated, under which in the event of a large-scale disaster or significant system failure, a task force consisting of General Managers and management will be set up based on the Business Continuity Plan (BCP), and under the instructions of the task force, service recovery operations will be carried out by the business functions responsible for recovery, with results reported to the task force. |
| § 164.310 (b) | Workstation Use | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | For personnel to operate Kintone, they must log in using a dedicated operational terminal, through the company-wide authentication infrastructure, which has appropriate access rights set for each employee, and SSO, and after logging into the AWS Management Console, they must go through the Bastion. Communication between the Operation Terminal and the Management Console, and between the Management Console and the Bastion, is encrypted. |
| § 164.310 | Workstation | Implement physical safeguards for all | Dedicated operational terminals that access the Kintone service |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| (c) | Security | workstations that access electronic protected health information, to restrict access to authorized users. | environment are installed in the server room where area access entry/exit are controlled by surveillance cameras, and taking dedicated operational terminals out of this area is prohibited. Additionally, important security events are monitored by an Endpoint Detection and Response (EDR) solution, and all operation logs are collected, ensuring deterrence against fraud as well as traceability in the event of an incident. |
| § 164.310 (d) | Device and Media Controls | Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility. | At Cybozu, the use of removable media for storing ePHI is prohibited. Furthermore, customer data stored in Kintone is automatically and completely deleted after a retention period of 30 days from the cancellation date. Note that the internal controls related to the physical and logical deletion of data within the Kintone service environment are maintained by AWS, and are therefore excluded from the evaluation. |
| **Technical Safeguards** | | | |
| § 164.312 (a) | Access Control | Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). | Accounts for Kintone development and operation personnel are assigned to roles with the necessary permissions for project execution in accordance with the Account Management and Account Management Structure procedures. The management of individual roles set for each AWS account and the personnel belonging to those roles is managed using a ledger. When an employee resigns or their contract ends, access rights to the assets and systems granted to them are returned or revoked based on a process with defined procedures. A list of the items loaned to the employee that are to be collected back from them and a process for |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | | changing access rights during employee leave of absence, or when they resign, have also been established to prevent any inappropriate accounts, access rights, or authentication devices remaining.<br>When an employee has resigned, the Service Desk department deactivates their account in the company-wide authentication infrastructure, which disables SSO to the AWS environment used by Kintone, revoking all access rights of the resigned employee. The account deactivation process is recorded and checked by a different person from the operator. |
| § 164.312 (b) | Audit Controls | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | At Cybozu, the Change Management Rules stipulate the procedures for work that involves making changes to an environment, rollback procedures, the creation and review of procedure documents, and the acquisition of records during change responses.<br>Operational tasks are carried out using a dedicated operational terminal, and all operation screens of the Operation Terminal are recorded.<br>Additionally, since the development and operation of Kintone fall under the scope of the Information System Management System (ISMS), internal audits are conducted annually in accordance with the ISO/IEC27001 standard. |
| § 164.312 (c) | Integrity | Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. | For personnel to operate Kintone, they must log in using a dedicated operational terminal, through the company-wide authentication infrastructure, which has appropriate access rights set for each employee, and SSO, and after logging into the AWS Management Console, they must go through the Bastion. All operation screens of the Operation Terminal are recorded. |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | | Furthermore, in terms of operational tasks, the release of applications with changes to external specifications or new features is managed and automatically deployed to the production environment via the release management system after approval from the PM. When manual intervention is required, the development team creates documentation detailing the response, conducts a review as stipulated in the *Yakumo Operation Rules (Manual Procedures)*, and records the confirmation of completion of the response. In the case of manual intervention, the rules stipulate a two-person process involving one person who does the work (Implementer) and a second person who verifies it (Checker). |
| § 164.312 (d) | Person or Entity Authentication | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | Access to the Kintone service environment is via SSO from the company-wide authentication infrastructure, which has appropriate access rights set for each employee. Additionally, as part of the account management policy, passwords must be at least 12 characters long using a combination of alphanumeric characters, and multi-factor authentication is set as mandatory. Also, in the event of authentication failure, automatic lockout occurs.<br>Furthermore, for personnel assigned to each permission set in the service environment, the person responsible registers the monthly inventory as a task and performs the inventory, and the checker reviews the inventory results. |
| § 164.312 (e) | Transmission Security | Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications | Kintone has implemented the managed threat detection service Amazon GuardDuty, which detects threats based on unauthorized operations, unauthorized logins, threat information, and behavior, and emails from GuardDuty are checked daily. When an alert email is received or specific |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | network. | warnings or errors occur during monitoring, alerts are communicated to personnel via the specified reporting method and addressed promptly.<br>In relation to system vulnerability monitoring, in addition to vulnerability assessments by the internal Cy-PSIRT, periodic vulnerability assessments are conducted by a third-party security vendor. Details of the initiatives and the annual assessment results are disclosed on the Kintone Corporation website.<br>In relation to the protection of communication data, customer data stored in Kintone is encrypted using AWS features (such as AWS RDS, S3), and access from user devices to Kintone is encrypted and protected by HTTPS protocol. |
| **Organizational Requirements** | | | |
| § 164.314 (a) | Business Associate Contracts or Other Arrangements | (i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.<br>(ii) A covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3).<br>(iii) The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § | Cybozu provides a Business Associate Agreement (BAA) for customers subject to HIPAA who use Kintone, such as customers in the healthcare industry. If you wish to enter into a BAA, you will need to check Cybozu's BAA and agree to it.<br>In addition, Cybozu has entered into a Business Associate Agreement (BAA) with its subcontractor AWS, and regularly checks the HIPAA compliance of the AWS services it uses and the details of AWS's security measures. |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate. | |
| § 164.314 (b) | Requirements for Group Health Plans | Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | Internal controls related to a group health plan should be established by the Covered Entities, so they are excluded from evaluation.<br>However, a CSIRT has been established as an organization to respond to information security incidents related to Kintone, and a system is in place for receiving inquiries, responding, and contacting relevant parties. |
| **Policies and Procedures and Documentation Requirements** | | | |
| § 164.316 (a) | Policies and Procedures | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies | The basic security policy at Cybozu, which includes the development and operation of Kintone, is reviewed under the responsibility of the Information Security Management Officer annually and whenever significant changes occur. |

| ID | Category | HIPAA Standard | Kintone Compliance Status |
|---|---|---|---|
| | | and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart. | |
| § 164.316 (b) | Documentation | (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. | All documents related to information security are stored in an internal system, and all versions are kept for at least six years.<br>Documents used on-site are revised as needed based on the judgment of the on-site manager, while company-wide regulations are discussed and revised by a meeting body that includes management.<br>In addition, if there are revisions to, or deletion of, the documents, employees will be notified through company-wide notifications and security training. |

## Points to Note

This white paper applies only when Kintone Corporation is a Business Associate or Subcontractor of the customer under HIPAA. The internal controls related to Kintone's security are one part of the internal controls regarding the use or other processing of PHI through Kintone by the customer.

When using this white paper, it is necessary to consider the complementary internal controls that should be established by you and your subcontractors.

Examples of key points to note are listed below.

Complementary internal controls to be established by the customer

· Internal controls for the use or other processing of PHI by the customer as a Covered Entity or Business Associate.

Examples:

- Controls regarding the management of Kintone accounts, passwords, and permissions to be granted
- Controls regarding the network security of client terminals
- Controls regarding customization using Web-API
- Controls regarding data backup for data recovery due to issues caused by the customer entity
- Controls regarding the physical handling of PHI
- Controls regarding offline storage of data
- Controls regarding user authentication for medical devices
- Controls regarding the transmission of ePHI via email; and
- Controls regarding other Covered Entity operations.

Complementary internal controls to be established by subcontractors

· Complementary internal controls that are expected to be established at AWS.

Examples:

- Controls regarding physical access to data centers
- Controls regarding the physical and logical deletion of data

- Controls regarding encryption of stored data
- Controls regarding the detection and reporting of system failures
- Controls regarding data backup and recovery
- Controls regarding change management of infrastructure platforms