CHINO.IO

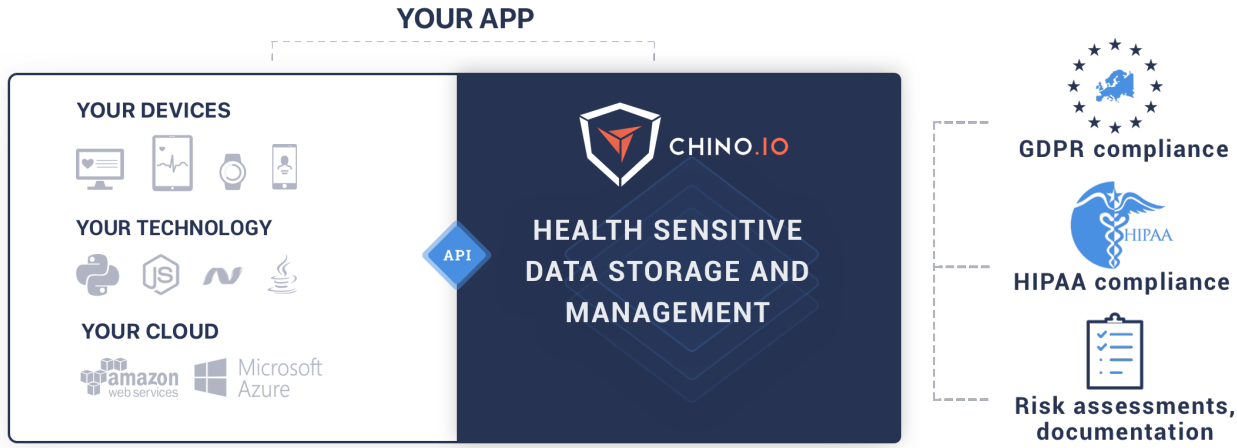
Chino.io Platform Security

Features & Guarantees

The Chino.io Platform

Introduction

The Chino.io Platform exposes a **standard, interoperable and secure API** to **manage storage of health sensitive data, users registration, authentication and access control policies (permissions) to health data.** The API is based on REST principles and enables developers to solve compliance and security issues, without disrupting their applications, technology or service delivery.



Chino.io **encrypts** data both in **transfer and at rest (at single record level)** and it hides the security complexity from developers. Data is encoded as JSON documents and can contain any content type like integers, strings, dates, lists, base64 encoded content, and binary attachments.

The API is extensively documented and Chino.io provides tutorials and SDKs to speed up the integration and application development. For more info about Platform check here: https://chino.io/api-and-docs

By using Chino.io platform and API developers can easily ensure compliance with EU and US data protection laws (GDPR, HIPAA, national requirements etc.). In addition, they can meet the demands and requirements from their partners and large companies, which frequently is more challenging that ensuring compliance of data protection laws.

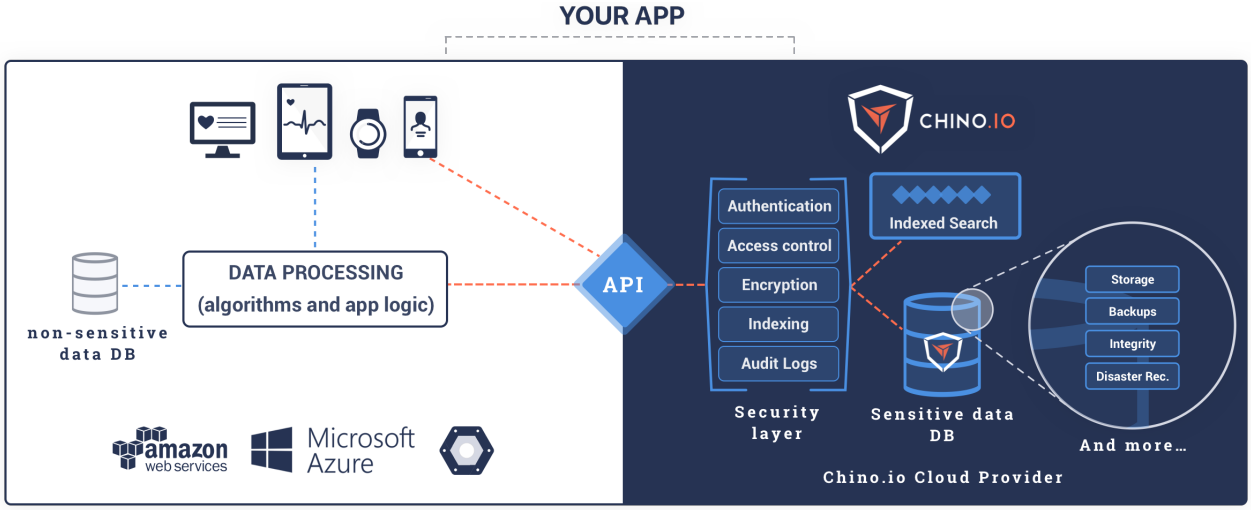
This White Paper focuses on security aspects, while to learn more about compliance requirements and how Chino.io handles and solves them for developers check

DOWLOAD CHINO.IO EBOOK ON HEALTH APP COMPLIANCE

The eBook highlights how Chino.io helps to ensure compliance with infrastructure/physical, technical implementation and administrative requirements.

The Chino.io Platform Architecture and Security

The Chino.io Platform is designed to outsource the majority of tasks and the complexity regarding health data security and compliance.



The main components of the Chino.io Platform are:

- **The API:** is the end-point that handles data, user management, permissions etc. It implements the data **security in transfer** (HTTPS) and security monitoring of all API operations in real time (attacks, errors etc.). The 24/7 **monitoring** system notifies the system administrator in real time when erroneous conditions are detected in the system. These real-time monitoring technologies are also developed in innovation projects with large companies and research centers, in which we exchange data about **real-time cyber risks and attacks** with National institutions and big companies like BT, SAP, HP, CEA etc. (for more info check www.C3ISP.eu). In addition to security, the API applies also techniques to ensure high level of **scalability** and extremely **fast execution**, giving responses to each API call in milliseconds. The REST standard ensures that the API can be used with your favorite language. We provide also SDKs in Python, Java, .NET and more to come. In particular the data management API are inspired by well-known standards and concepts typical to noSQL databases (e.g. MongoDB). This makes it easy to start developing on Chino.io API and doesn't create lock-ins in our technology.
- **Authentication**: to Chino.io API is done via access keys (CustomerID and CustomerKey) or via end-users' usernames and passwords using OAuth 2.0 protocol. Access keys method uses basic auth and keys represent the username and the password, thus they require to be stored in a safe environment, e.g. the OS Keychains (as explained in our guidelines). Access keys

can be generated or invalidated at any time from Chino.io Console. If Chino.io database is hacked the data cannot be accessed since the records are encrypted. To decrypt the data the malicious user must posses the user's data encryption key and the master key, which requires to gain access to different environments and VMs that are protected with various keys and access permissions. security starts with strong authentication.

- **Access Control** (or Authorization): access control policies (also called Permissions) provide a very granular and flexible, and are defined via our API. In this way, developers have certainty that users can perform only authorized operations on data. The policies can be setup via the API to define access rights for single users or groups of users to single documents or collections of documents (Repository, Schema, Document, UserSchema).
- **Encryption:** Chino.io encrypts data in transfer and at rest at single record level (or also called application level). Each API call uses HTTPS/TLS encryption, all documents are encrypted at rest and at record level using AES-256, passwords are stored with PBDKF2 algorithm. The virtual machines have enabled encryption at disk level, regular backup are executed on the database, on the blob files and log files, all backups are encrypted and stored in a different physical location respect to the server where the VMs are. Each Chino.io customer has different data encryption keys that implement a multi-tenant environment. Encryption keys are stored in separated environments and VMs. Encryption keys are accessed applying concepts of HSM - Hardware Security Modules. User's data-encryption keys are encrypted using a dedicated key for each user. A Master Key is used to re-encrypt all the data, thus, both keys are needed to decrypt and access the data. **The overall Chino.io encryption approach drastically improves the standard cloud providers' offers**. For example Amazon AWS and Microsoft Azure provide database level encryption on disks **and are not responsible for your data.** Check here the AWS and Chino.io shared responsibility models for a comparison.
- **Indexing:** storing data without having the possibility to search it in milliseconds would be useless. Chino.io allows you to index certain fields of Documents to make the search operation extremely fast. Chino.io applies tokenization techniques to ensure a fast and high availability system that support our Search operations. Chino.io tokenizes only the data that requires indexing, without storing the other document fields, and encrypting the tokens at rest on the disk. When you search a document, the search operation returns only the document ids. The corresponding documents are retrieved encrypted from the database, decrypted, and forwarded to you via HTTPS in milliseconds.
- **Auditing:** all operations are audited in a legally valid immutable logging system. The system tracks who accesses your data, when it was accessed, and from where. Currently Chino.io is

working on blockchain technology on these aspects, to provide you and your customers even more trust.

- **Encrypted Data Storage:** data and backups are always stored encrypted using AES-256 algorithms. Backups are created and transferred to a different physical location.
- **Backups and Disaster Recovery:** we do daily incremental backups on the database. Backups are stored in two separate physical locations. We keep a full week backup history, plus four backups for the current month (each Monday) and one backup for each month for 6 months (first day of the month). Blobs are stored using Google Technologies that backs up the data autonomously. Note: Blobs stored on Google are encrypted. We do also full system backups of VMs and setups and we perform tests on backup validity and recovery procedures on regular basis. The Chino.io components are containerized and the deployment process is orchestrated automatically in case of discovered failures. This defines also a reliable Disaster Recovery procedure that prevents service outages.
- **Access to data:** technically Chino.io team has access to data, however, this never happens in practice since there's no maintenance cases that require the team to decrypt the customers' data. Moreover, accessing the data requires to have in hand master keys, which are set in a special VMs and that only the CTO and CEO have access (we do have to keep a access to allow users to recover the data in case they loose access keys or password). Any access to the Chino.io platform is logged and the permissions of system administrators are managed centrally by Chino.io CEO and CTO. Chino.io has a criminal law responsibility for its customers' sensitive data according to the EU data protection laws and Italian jurisdiction.

Data and Platform Location

For non-HIPAA compliant customers Chino.io platform uses Hetzner Online Gmbh dedicated hosting provider which is located in Germany. Chino.io team implements and manages virtualization, scalability, replication and all other aspects of cloud computing.

For HIPAA compliant customers Chino.io relies on Google Cloud Platform located in Frankfurt, Germany, which provides all necessary guarantees at infrastructure level (IaaS). However, due to specific requirements of some of its customers or EU member states, Chino.io provides also ad-hoc installations of its service in any cloud.

In any case, the Chino.io cloud instance will be always located in Germany due to the interpretations of German data protection law and our current customer base.

Different Regulations and Cross Border Data Transfer

Chino.io is currently compliant with the EU, German and US/HIPAA regulations. To comply with national certifications like the French one, Chino.io is working with local hosting providers to create different instances of its service. The current cloud Chino.io installation for current customers will always stay in Germany.

How Chino.io deletes my Data

When you delete something via APIs, it is deleted from our database and the indexing service. When you delete your account, Chino.io deletes all your data and your encryption keys and therefore all data can't be accessed anymore even from backup copies, implementing the Right to be Forgotten guidelines introduced by GDPR using most conservative approaches..

How Chino.io protects PII information?

Chino.io implements all technical safeguards to protect health data according to the highest security standards and US/HIPAA and EU/GDPR data protection laws. Following its commitment to security and quality Chino.io is also certified ISO 9001 and 27001.

How Chino.io applies OWASP TOP10 cases

OWASP cases relate mainly to the Web and API, and for us the API security is fundamental. For more information check the previous sections on Chino.io Platform description.

How Chino.io installs security updates?

We always keep our system and your software up-to-date in terms of security standards and updates (e.g. 0-day vulnerabilities). Major updates are notified via email to our customers in advance.

How Chino.io ensures compliance?

Compliance with EU and US data protection laws is a fundamental goal and mission of Chino.io service and company. For more information check related resources:

- Chino.io Compliance Webpage
- eBook on Health Apps Compliance

How Chino.io supports developers on documentation?

Chino.io helps also on administrative and documentation requirements by providing documentation to help developers to document, certify and prove compliance of their applications. For example, Chino.io provides Security Risks Assessments that developers can use to demonstrate security of their applications to users and customers. This documentation is shared with all customers once the on-boarding process is completed.

In case I stop using Chino.io, how can I download my data?

Just contact us, we will help you in downloading your data in bulk. You can always download your data by using our API.

For billing and account termination details please check our Terms & Conditions.

How Chino.io manage the due diligence?

Chino.io manages everything internally, except from the computing infrastructure which is provided by Google Cloud Platform node in Frankfurt.

Can Chino.io access to my data?

Since Chino.io manages encryption keys, there is technically the possibility that it could access to data. However, this is typically never the case and we comply with best standards when it comes to internal policy definition, management and implementation of access procedures.

Chino.io complies with ISO 27001 and HIPAA security guidelines when it comes to security procedure implementation.

Only system administrators have access to the Chino.io VMs that manage encryption keys.

How Chino.io exchanging hard discs?

Infrastructure level security and management is performed by Google Cloud Platform, which is EU law and especially HIPAA compliant.

GCP Security White paper: https://cloud.google.com/security/whitepaper

Who has access to the production system?

Only system administrators of Chino.io. To access VM and containers on the GCP we rely on the Google access control system, adding users (our employee) to the different resources they may have to access.

Is access to the production system traceable?

Yes, every access to VMs, DBs and code is tracked and part of the audit log.

The team is notified via different communication channels each time there is an access to data (or unauthorized access, outages, system capacity etc.).

Google cloud platform offers instruments to have audit logs (e.g., https://cloud.google.com/logging/docs/audit/)

How and when do we get information about a potential incident?

Chino.io is liable according to the Breach Notification guidelines to notify its customers about any breach or incident.

In addition, audit logs are stored in immutable data structures, which provide legally valid proof in case of need.

If our solution needs to be penetration tested, do we need to inform you about it?

Yes, please inform our team about penetration testing in place. Typically, this should be done on our Testing/Sandbox environment, which provides an almost exact copy of the production environment.

Who does the audit of Chino.io and what are the audit frequency?

ISO certificates have 2 years validity (check later), with intermediate yearly inspection and progress reporting phases. The certification body is named “QS - Quality Services LTD” and it’s accredited by Italian entity for accreditation Accredia.

Is Chino.io certified?

Chino.io applies certifications that are common to nowadays service providers to demonstrate quality and security best practices:

ISO 9001

ISO 9001 is a quality management standards and it specifies the best practices and mandates the implementation of a proper Quality Management System (QMS) within a company.

With the ISO 9001 Chino provides the necessary guarantees and documentation for building medical grade software that needs to undergo the CE marking or ISO 13485 certifications.

ISO 27001

ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. It includes the development and implementation of a rigorous security program, an Information Security Management System (ISMS) and how Chino manages security in a holistic, comprehensive manner.

Chino's implementation of and alignment with ISO 27001 demonstrates a commitment to information security at every level of the organization. Chino is assessed by an independent third-party auditor to validate alignment with the ISO 27001 standard.

Chino.io Platform and API Technology

What is an API call?

Every time your app stores or retrieves some data, or a user logs in or out, your app performs one or many API calls. We count only authenticated calls. Unauthorized calls are not counted, while wrong calls (i.e., incorrect formats) are counted.

The number of calls that you need highly depends on your implementation. Check out "Tutorials" to find out how you can use our service.

How many JSON documents can I store in 1GB?

We count 1 byte for every char in the document body (we do not count document metadata, only the content).

This means that the Divina Commedia (which has 408.476 chars, space excluded) can be stored in ~500 KB. You can store it up to 2000 times. If you store BLOB, then keep reading.

How many BLOB files can I store in 10GB?

We count the byte size of the attachment you send. The Divina Commedia has ~700 pages. If we assume that a scanned page is ~500KB, the whole book is 350MB. In 10GB you can store 35 scanned copies (the biggest problem is how to scan 700 pages).

How can I determine how many calls my app consumes per user on average?

You can do it by counting how many operations over data you need to perform per each user session. Then you add a couple of calls for logging and logouts operations.

You can always monitor API usage on Chino.io Console.

How can I store files larger than XX GB?

Each BLOB can be up to 1 GigaBytes. You can upload BLOB documents by using our chunked upload function. You can decide the chunk size based on your device capabilities and network reliability (each chunk must be transferred within an https call).

How many users can my app support with each plan?

For security reasons we limit the number of users to 100.000. If you need more, just contact us.

How many repositories and schemas can I create?

For security reasons we limit the number of repositories and schemas to 1.000. If you need more, just contact us.

Can I transfer my app to someone else?

Yes. You just need to update your personal and billing data in Chino.io Console.

How can I grant access to the API to other people?

You can grant access to the API to other people in 2 ways:

- If you want to give admin access to someone you just need to generate another Customer Key and share it with whom you wish. You can delete/invalidate that Key later on.
- If you want to give access to someone only for specific repositories/schemas/documents through API, then you can create a User and setup Access Control policies for him.

Can I get Chino.io deployed on my own server?

Yes, this is one of our custom deployment options. Since it requires a dedicated instance and dedicated management of the installation and monitoring, the pricing is provided ad-hoc based on your needs. Just contact us for more details!

Does Chino.io offer SLA's? (Service Level Agreements)

Yes, Chino.io does its best to guarantee the highest level of service uptime of at least 99.9%. In case of incidents Chino.io clearly states ranges for reimbursements. For more details check our Terms & Conditions.

9001

27001

FIND MORE INFO AT:

www.chino.io / info@chino.io