A brief guide to the compliance of health apps in the EU

What developers need to know about data protection, and how Chino.io helps them

Abstract

Digital health services are disrupting the healthcare sector by injecting huge innovation, improving the quality of care and strengthening the doctor-patient relationship. However, by their very nature, such services collect and manage extremely sensitive data and therefore need to comply with security and privacy requirements defined by data protection laws.

For application developers tackling privacy and security represent a huge challenge. To develop the technology for managing collected data in accordance with laws represents a painful, costly, and potentially extremely risky activity due to the possibility of data loss, thefts and penalties.

Moreover, the EU legal framework is very fragmented and rapidly evolving. This makes it very difficult to understand, not to mention extracting and implementing data protection requirements to ensure compliance.

This brief guide gives an intro to the regulations, key challenges for developers, and shows how Chino.io can help developers to build secure and compliant health applications.

Index

Healthcare is going to the cloud

Cloud computing is being adopted both by hospitals and by Digital Health services (mHealth, eHealth, Connected Devices etc.), which are cloud-native by definition, and are increasingly integrated into healthcare processes used by providers and citizens.

At present there exist circa 260.000 mHealth applications worldwide (100.000 more than 2015), 60% of them are developed by SMEs and startups, while 40% are located in the EU[1]. The result is:

"92% of healthcare providers are already using one cloud service"

Due to this trend, huge amounts of health data is now stored and transferred **outside of the physical borders** of hospitals. This course will be exponential in the coming years (Digital Health CAGR is ~30%).

The **transition to cloud represents a big challenge** for all actors involved. From governments defining new laws and standards to hospitals adapting their procedures and systems to individual application developers who need to deal with new responsibilities.

Why cloud computing represents a big challenge for service developers

We identified two main reasons when working with entrepreneurs and companies globally:

1. The **legal responsibility** for managing health data is **transferred** to **service developers, i.e. the CEOs of startups and companies**. That means: if you are a CEO, you need to be up to speed on privacy laws and regulations, because you will be legally liable for explaining to users privacy policies and implementing data collection and processing according to applicable laws. This is extremely challenging and risky in the EU since the legal framework is very fragmented, complicated, and evolving; **sensitive data management is criminal liability punishable with strict fines.**
2. The **technical responsibility** for service delivery is **completely transferred** to **service developers**. In the pre-cloud era services were usually physically deployed in hospitals' servers and hospitals were managing the infrastructure while developers were liable only for maintenance. Instead, in cloud era developers bear complete **responsibility** for the

[1] https://ec.europa.eu/digital-single-market/en/public-consultation-green-paper-mobile-health

infrastructure, service maintenance and delivery, **data and system security**, Quality of Service (QoS), and **Service Level Agreements** (SLA).

Those aspects are equally important whether the final users are citizens (B2C companies), or big organisations like hospitals, pharma companies or insurers (B2B companies). In the first case developers must sign contracts with citizens (privacy policies and terms and conditions), while in the other they sign contracts with corporations (contracts, security risk assessments).

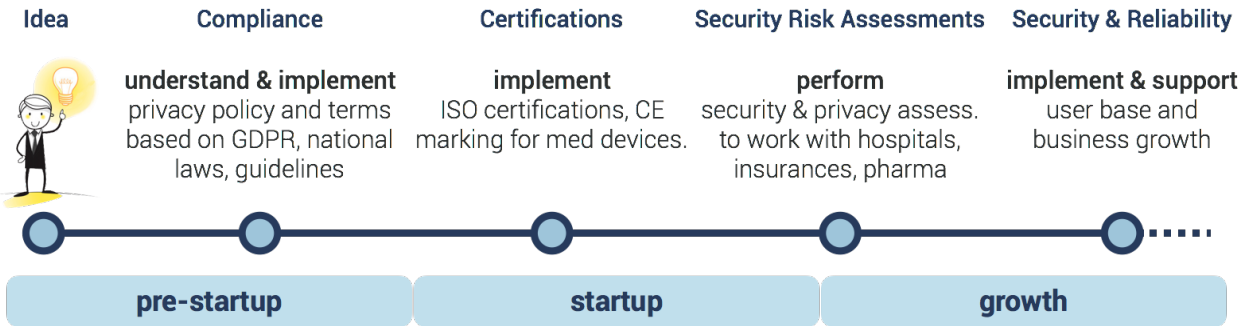
How are developers dealing with this?

Very poorly. According to studies performed from 2014 to 2016:

- **85% of apps** do **not display a privacy policy properly**[2]
- **66% of apps** approved by NHS App Library do **not use secure protocols (i.e. HTTPS)** for transferring health data[3],

Given the value of health data and the potential harm to end-users, **governments started investigating the behaviour of apps**[4]**. This in turn led to** regulating apps at national levels[5],[6].

By working with different companies we observed their **difficulties and challenges at each phase** of product creation, from design to, commercialisation and growth.



Typically each startup phase, from idea to growth, brings different challenges:

- **Compliance:** the **analysis** of **legal** aspects is usually the first steps that a company has to do to **learn** about **privacy, security and managing health data.** The analysis involves the definition of privacy policies, terms and conditions and overall product design. The design

[2] http://www.bbc.com/news/technology-29143107

[3] https://www.theguardian.com/society/2015/sep/25/nhs-accredited-health-apps-putting-users-privacy-at-risk-study-finds

[4] https://arstechnica.co.uk/tech-policy/2016/11/fitbit-jawbone-garmin-mio-norway-privacy-complaint/

[5] https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised

[6] http://medicinadigitale.it/2015/08/24/mobile-health-il-ministero-istituisce-un-gruppo-di-lavoro/

aspect has been emphasised especially with the new EU General Data Protection Regulation (GDPR) which introduced the "**Privacy and Security by Design**" concepts as fundamental requirements and best practice in service development.

- **Certification:** this is probably the most impactful challenge for digital health companies, especially in case of **medical grade devices or software** which requires CE Marking (or FDA approval in US) of classes II (a, b, etc)[7]. Getting a certification can heavily impact company timeline and budget. The certification process also involves documenting and guaranteeing product quality, security and data protection.
- **Security Risk Assessments:** these consist of complex checklists about security and product quality that a company must sign in form of **contractual obligations** to work with a **hospital or a large company**. This is usually done at a stage when the product is developed and ready for the market. For a company meeting the necessary requirements, and potentially modifying its product, can be extremely challenging and costly.
- **Security & Reliability:** these are essential to support the growth stage which usually brings new challenges regarding product stability, quality and overall security. Typically, in this phase companies must ensure scalability and security, which is very challenging.

Since these challenges are related to the company/product maturity and growth stage, **the later they are encountered the bigger impact they cause to the company**.

Risks and impacts on companies for non compliance

With low quality applications and higher risks, as perceived by end users, the impact could be immense for the entire digital health sector. In particular:

- **Loss of trust** in digital health products: recent studies shown that 59% of people don't like sharing data online, other studies criticise applications ability to deliver promised benefits.
- **Penalties and business risks** in case of hacks or accidental data losses. With the GDPR the fines for the non compliance and the misuse of personal data have been increased up to **20M Euro or 4% of global company turnover.**
- **Harder proof of compliance** in order to sign partnerships with public and private larger institutions. This is also given by the fact that new laws and requirements are being introduced at EU and single state levels.
- **Less innovation** due to the introduction of higher barriers, standards and certifications that affect mainly small players who don't have enough resources. This difficulty has been observed already in countries with strict national level certifications such as France who introduced the HDS certification for hosting providers (see later for more info).

[7] https://ec.europa.eu/growth/sectors/medical-devices_en

How to ensure compliance in the EU

The first question developers need to answer is whether their applications collect health data.

The key question: what is health sensitive data?

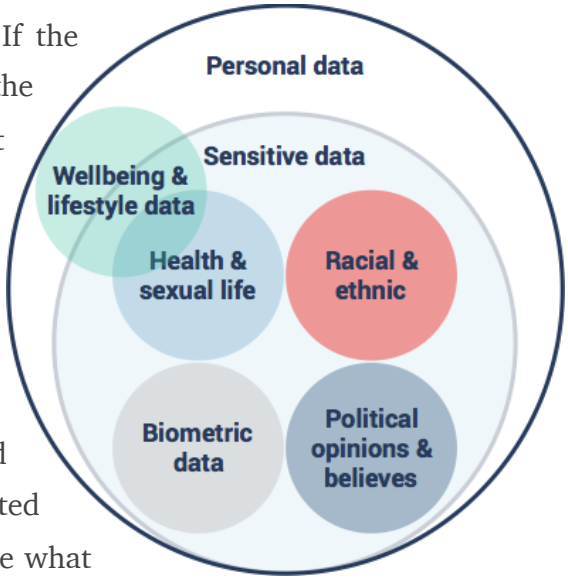
The short answer is: **it depends**. The key to answer this question is to **understand** whether the data **reveals the health status** of a person or not**.**

The new EU General Data Protection Regulation (GDPR) is extensive (but not exhaustive) in its definition: "*all data related to the health status of a subject and is collected for the purpose of deducting the health status of someone*". The Article 29 Data Protection Working Party, an EU body with advisory status, provides a more detailed definition, which defines **health data as**[8]:

- **Medical data** providing information about the physical or mental health status of someone (the data subject), generated in a professional medical context.
- **Raw data** collected by apps or devices that can be used to induce, individually or aggregated with others, someone's health status or health risk.
- **Data that can permit someone to deduce a person's health status or risk**, regardless of the accuracy, legitimacy or adequacy of this deduction.

Although this classification seems clear, there are still "grey areas", like in case of wellbeing apps, where the classification is often extremely difficult to interpret.

Example: A fitness app that counts a person's steps. If the data cannot be combined with other data, and if the specific medical context in which the app is used is not available, then it is non sensitive data. If the data can be easily combined with other data-sets, however, it can become sensitive data. If it, for example, is combined with heart rate, or compared with data from other people, it can reveal sensitive information about a person's ability to perform stressful activity, and thus stretches into the sensitive health-category depicted above. As you can see, it's not always easy to determine what constitutes sensitive data or not.



[8] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

The EU legal framework for health data protection

If an application collects health sensitive data it must ensure compliance with the EU data protection laws. This is extremely challenging and it requires a strong knowledge of EU and national regulations, and most of all a significant amount of time and resources.

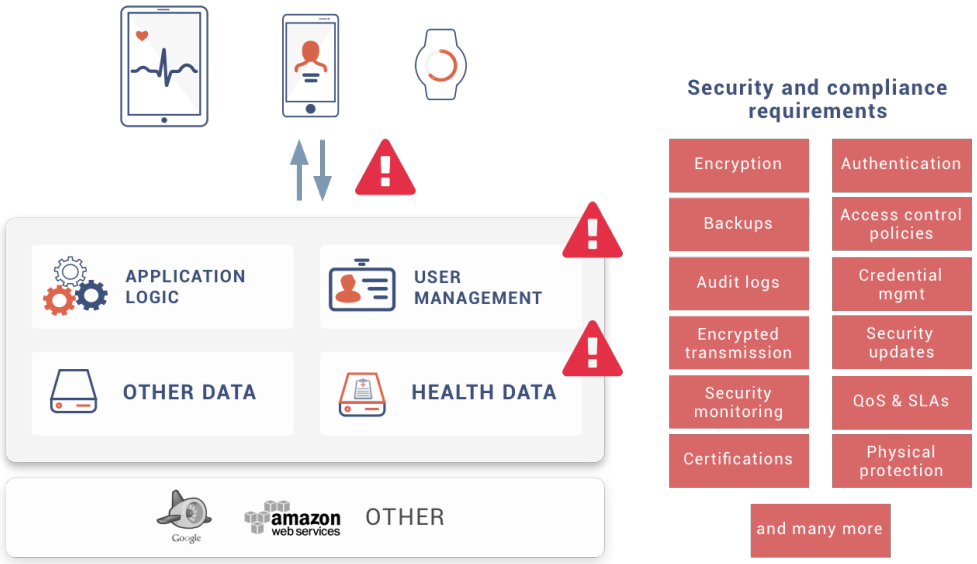
The table below summarises the different requirements that developers need to consider:

 **EU Laws and Directives**	**EU Data Protection Directives and Regulations.** These include also Article 29 Working Party opinions and recommendations (soft laws), EU Court of Justice rulings (e.g. invalidation of Safe Harbour). They are usually high level laws that define rules and principles on data processing and service delivery. The new General Data Protection Regulation (GDPR) defines also strict penalties for not compliance and stricter rules for data processing.
 **Cyber Security Standards**	**EU Cyber Security Regulations and international security standards.** These are defined also by organisations such as ENISA, OWSP or ISO (e.g. ISO 27002 controls). They define more technical requirements, controls, security principles, and quality management principles that must be applied during software development.
 **National Laws and Requirements**	**Individual countries' data protection laws and standards.** Each EU member state, and sometimes even single regions (e.g. in Germany), define rules and requirements for healthcare sector and apps. Mostly these rules affect only those working with public bodies in healthcare sector, while in others they apply to any service dealing with health sensitive data.
 **Certifications and customer specific requirements.**	**Specific regulations for medical software and clients requirements.** Although these are two very different categories, they usually demand developers to provide heavy documentation and proof that quality and security levels have been met before delivering the service. CE Marking and security risks assessments, privacy impact assessments, terms and conditions, etc., are all part of the documentation and quality management processes that are implemented by a company.

Data protection requirements for developers

The list of legal requirements is long and very difficult to process — even for large organisations. Here we give a brief overview of what developers must consider from an infrastructure, technical, and administrative points of view:

- **Infrastructure:** developers must choose an infrastructure provider that satisfies all EU rules for processing and storage of sensitive data. This includes such things as reliability (i.e. SLA), clarifies hosting liability (with the new GDPR - Data Processor rule), physical infrastructure protection, certifications (depending on member state). **NOTE: there are no EU laws that restrict the location of data to one specific state.** But organisations tend to limit storing data to specific states or the EU physical borders.
- **Technical**: as depicted in the figure below, a typical cloud application has different components on the backend side that are responsible for the user, data, and application logic management. The list of technical safeguards affects mainly the API, user and health data. They include developing authentication, access control, encryption of data in transfer and at rest (storage), secure audit log, security monitoring and updates, backup, and reliability (QoS and SLA). Implementing these technical requirements demands a huge amount of work, knowledge, and time to ensure that all requirements and controls are met and that an application is ready to work with hospitals or other partners. **They are typically included in the Security Risk Assessments and contracts that developers must sign.**



- **Administrative**: need to be considered case by case involving lawyers and privacy experts. Developers must ensure their data processing is legal and that their service is properly regulated within terms and conditions. They must collect users' explicit consent, notify the data protection authority, define website privacy policy, perform security risk assessments, and certify the company and product depending on the nature of your health application.

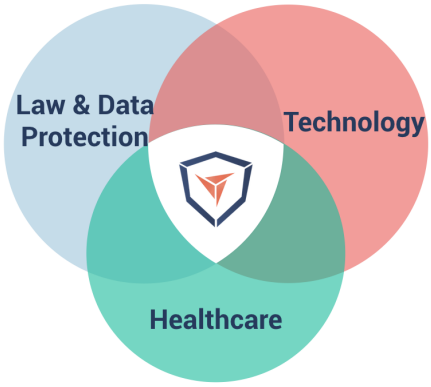
How Chino.io helps developers

Chino.io has created a development Platform with the mission to:

"Enable digital health application developers to build secure and compliant applications and deliver them globally — without legal or technical barriers."

With the Chino.io Platform developers can **easily build any kind of digital health applications and easily store and share health sensitive data in compliance with EU regulations**.

The Platform, originates from Chino.io founders' 7+ years of experience in the healthcare industry. Chino.io's **team combines experience from law, technology and healthcare.** We continuously collaborate with companies, lawyers, and operators all over the globe to understand their needs and help deliver better services.



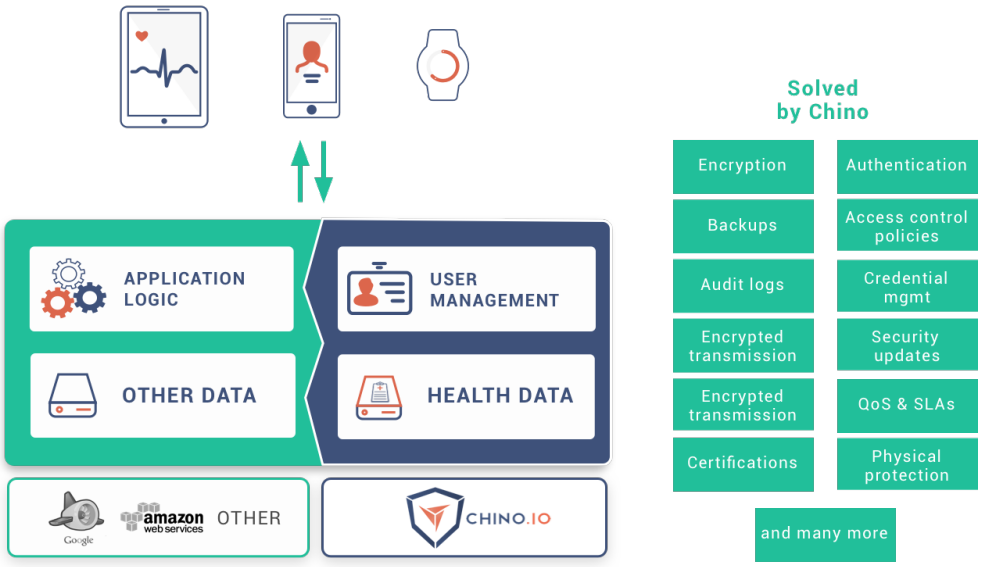
The Chino.io Platform

The Chino.io Platform exposes a **standard, interoperable and secure API** to **manage users registration, authentication and access control 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. Data is encrypted both in transfer and at rest and, hides the security complexity from developers. Data can be of any format, either structured JSON objects or binary attachments (also called BLOBs).

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

The Platform solves compliance requirements as follows:

- **Infrastructure**: Chino.io relies on trusted cloud providers located in the EU (currently in Germany) which provides all necessary guarantees. However, due to specific requirements of some of its customers or member states (e.g. France - see later for future plans), Chino.io provides also ad-hoc installations of its service in any cloud.
- **Technical**: Chino.io implements all technical safeguards to protect health data according to the highest security standards and data protection laws. For more details about all technical features **see the Annex.** Following its commitment to security and quality Chino.io is also **certified ISO 9001 and 27001.**



- **Administrative**: although these requirements are specific to each application, Chino.io provides all the documentation to help developers to document, certify and prove

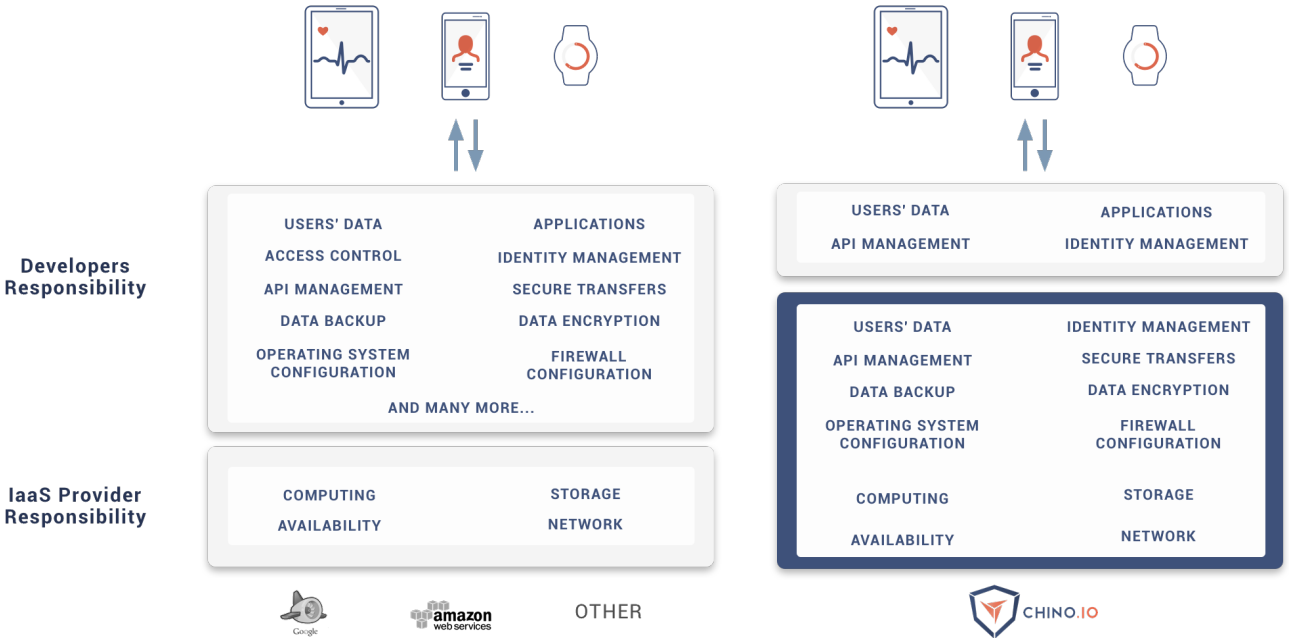
compliance of their applications. For example Chino.io provides Security Risks Assessments that developers can use to demonstrate security of their applications to users and customers.

Why use Chino.io

Security and compliance are not the only benefits. When compared to classical IaaS providers like Amazon AWS[9], Chino.io **shares the liability** of managing health sensitive data and application security because:

- its **required by the new EU GDPR**, and already applied in HIPAA in US and HDS in France (see next section for details).
- it **reduces risks** for customers who can delegate security and responsibility to Chino.io.
- help you in working with hospitals, insurers, and other big corporations, which demand security and liability. With our support you can gain trust with your partners and your users.

Classical IaaS providers **do not provide any liability regarding the data** that developers store.



However, it's important to notice that **application developers** do still **share part of the responsibility** of managing users' data, and overall application security. For example they are responsible of managing the API access keys, proper implementation and usage of the API within their applications and exposing the API to client applications.

[9] https://aws.amazon.com/compliance/shared-responsibility-model/

Case Study

blue by NEEDIUS technologies for special needs

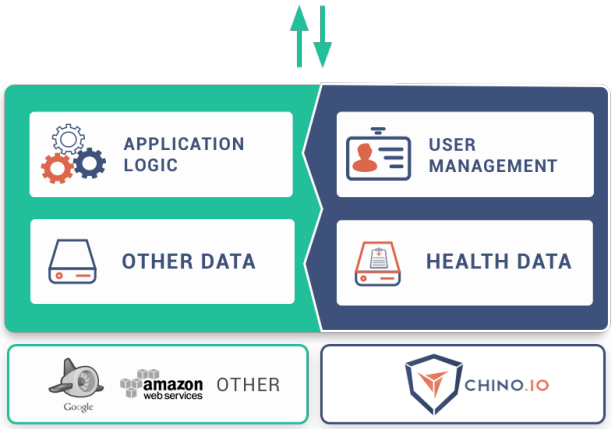
www.tabletautismo.it

Blu(e) is a communication tool for children affected by autism or other communication disorders which complicate the interaction with the external world. The platform provides also remote management and monitoring for users' supporting network (family and physicians).

Remote management system for physicians

Tablet usage by the user

Monitoring by physicians and family



Blu(e) collects health sensitive data and shares it among users on different applications. With the help of lawyers the company Needius defined security and privacy requirements, in addition to preparing a privacy policy. The collaboration with Chino.io helped to secure the data and overall platform and the resulting configuration regarding data storage is:

- **Blu(e)'s backend:** keeps the data about application usage which requires heavy elaborations.
- **Chino.io manages:** users profiles, user authentication and stores generated patient profiles which contain sensitive data. The data sharing and access control is done with Chino.io API.

The resulting configuration didn't disrupt the Blu(e) application logic and service delivery, and it has been approved by lawyers, who authorised Needius to deliver the services in the EU.

Chino.io compliance

To ensure compliance with EU current and forthcoming data protection laws Chino.io employs lawyers and has external collaborators across the EU. Chino.io already started working on the **GDPR**, the new EU Data Protection Regulation, which is a law already applicable and it will be mandatory for **anyone delivering digital services to EU citizens by May 2018**. The GDPR introduces many changes to the EU legal framework and one of them is the Article 24 which defines guarantees and responsibility that service providers must provide to developers. In particular the contractual relationship between providers and developers must clarify the liabilities regarding the specific processing.

Therefore developers must select providers which provide guarantees based on the risks associated to their application and data. As mentioned before, **Chino.io is already compliant with this specific article** since we clearly states in our terms and conditions that we manage health sensitive data on behalf of our customers.

This concept of **shared responsibility** is being already **applied in HIPAA in US, HDS in France,** and is being **introduced in the GDPR.**

In addition to the GDPR, at EU level Chino.io ensures compliance with the current Data Protection Directive (95/46/EC), ePrivacy Directive (2009/136/EC), EU Data Protection Supervisor guidelines for health data (Opinion 01/2015 on Mobile Health), Article 29 Working Party Opinions (Annex to the Directive 95/46/EC about health data in apps and devices (2/2015), Opinion 05/2014 on Anonymisation Techniques, Opinion 06/2014 on the legitimate interests of the data controller in Directive 95/46/EC, etc), and constantly monitors the forthcoming laws and regulations under approval.

Regarding **member states,** each of them already implemented the Directive 95/46/EC into national laws. The GDPR is also applicable in each EU state. As a result the **rules for processing sensitive data are uniform in all EU states**.

However, some states **introduced additional certifications** that defined further requirements for health related applications. For example HDS in France is a mandatory certification for data hosting providers for healthcare and biometric data. It states the security guarantees regarding the infrastructure management and it introduces the before-mentioned shared responsibility model between hosting providers and customers. Chino.io future plans include the HDS certification and HIPAA compliance.

Brief look at Chino.io's future

Following our vision and mission we are committed to help application developers to **deliver their services globally.** This means that Chino.io plans to become compliant with all major data protection standards and obtain required certifications.

Chino.io already acquired ISO 9001 and 27001 certifications and started working on HIPAA compliance for US market and HDS certification for French market in partnership with a large infrastructure provider. Updates on this matter will follow in Q1 2017.

Brief intro to **HIPAA**, the US regulation that governs the health sector and among other things it defines the legal basis for health sensitive data management among users, health operators and service providers. The HIPAA law is based on a shared responsibility model and it mandates to health operators (Covered Entities) to sign a Business Associate Agreement (BAA) with their service providers (IaaS, BaaS, SaaS). This creates a chain of responsibilities in which a SaaS provider must sign a BAA with its IaaS providers, and it must offer a BAA to its customers. This chain of shared responsibility gives more trust and security guarantees in managing health data, and Chino.io is already in line with such requirement.

Chino.io is also working with large companies such as BT, SAP, HP and academic institutions on the **forthcoming EU Cyber Security law** and on implementing the EU-wide network for real-time sharing of information about cyber attacks. More information will be available soon on our website.

In addition to legal and compliance evolutions, Chino.io is working on its Platform evolution from technology and features points of view. Features like end-to-end encryption and secure push notifications are some of the things we are working on currently.

Stay tuned!

for further info do not hesitate to contact us at: info@chino.io

Get compliant and secure with Chino.io

Chino.io Platform is **free** for development and it takes less than 10 minutes to start.

Learn how to get started at www.chino.io

ANNEX - Chino.io Platform security

These are the main technical features of Chino.io Platform:

Authentication
Security starts with strong authentication. We rely on standard OAuth2 protocol to implement authentication, and simplify the integration in a 2-ledged or 3-ledged fashion (OAuth as a Service).

Authorization
Flexible and granular access control 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.

Encryption
Each API call uses HTTPS/TLS to protect data transfers, while all documents at rest are encrypted using AES-256. Each user has different encryption keys, stored on different locations.

Backups
Daily backups of all data. Backups are encrypted using AES-256 algorithms and transferred to a different physical location. We perform backup integrity tests periodically to check if the recovery procedures work.

Active monitoring
Sleep well, we keep an eye (24/7) on what happens in our systems. Integrated real time monitoring notifies us always when something happens in the system. We are also working on a project (called C3ISP) in which we exchange data about cyber risks and attacks with National institutions and big corporates.

Secure audit log
Control who accesses your data, when it was accessed, and from where. Logs are legally valid and non-modifiable. We are also working on blockchain technology on this aspects, to provide you and your customers even more trust.

Secure cloud
We manage physical dedicated servers located in Germany on which we implemented virtualisation and parallel computing to offer scalability, reliability and high level of QoS and SLAs.

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).

Platform and API flexibility

These are the main features of Chino.io Platform regarding the API and its service:

Employ Chino.io with any technology
Our REST API can be used with your favorite language. We provide also SDKs in Python, Java, .NET and more to come. 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.

Try Scalability as a Service
Unlimited power at your service and control, scale when you need to. We will keep up at any pace.

Start for free no credit card required
Develop and test with no fee within our sandbox. Pay only when you are ready to go to market and real customers.

Use your own cloud
You can use any cloud for your computing. Move only sensitive data to Chino.io and forget data storage issues.

Chino.io certifications

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.io 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.io manages security in a holistic, comprehensive manner.
Chino.io's implementation of and alignment with ISO 27001 demonstrates a commitment to information security at every level of the organisation. Chino.io is assessed by an independent third-party auditor to validate alignment with the ISO 27001 standard.