healthware + INTOUCH SOLUTIONS®

MAY 2018 - POV

GDPR Compliance for Digital Health Startups

WHY DIGITAL HEALTH STARTUPS NEED TO WORRY ABOUT GDPR?

By their very nature, digital health applications collect a special category of data (also called sensitive), which is highly regulated and imply high legal responsibility, i.e. **the criminal liability for company representatives**.

Therefore, for digital health companies it's of fundamental importance to comply with all administrative and technical requirements defined by data protection laws such as the EU GDPR in order to reduce risks for data breaches, losses and other violations of users' privacy.

Some facts:

Fines: Violations of GDPR rules can cost to a company up to a 4% of its global turnover or 20 million Euro in EU and in the US the HIPAA regulation defines a fine of 225$ per each record that has been breached.

State of the art: According to studies performed in the last 3 years, developers are struggling with compliance. An 85% are not compliant and 66% do not use HTTPS. This behavior is putting at risk eHealth businesses, citizens' personal data, and trust in eHealth overall.

WHAT IS HEALTH DATA?

The Art. 4(15) of the GDPR defines "data concerning health" as: "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

Besides health, sensitive data category includes other types of data, such as the ones regarding racial or ethnic origin, political opinions, religious or other beliefs, trade union memberships, biometric which identifies a person, genetic, and offences/convictions information.

This definition is sometimes hard to apply to real cases of applications that are not purely health related, but rather wellbeing, wellness, or related to diet management or physical activity. In those cases developers may need to consult specialists to understand if their data is sensitive or not.

For more info you can check this short eBook: https://chino.io/static/content/Chino.io-Decision-Tree-on-Sensitive-Data.pdf

WHY FOR DIGITAL HEALTH STARTUPS IS SO IMPORTANT TO DEMONSTRATE COMPLIANCE?

Healthcare is characterized by a very complex set of stakeholders. Typically end users are not the customers. The customer can be a hospital, insurance, pharma company, or another public or private authority delivering services to citizens. To each of them startups need to demonstrate quality, security/compliance and trust.

Moreover, recent studies showed that 59% of people don't like sharing data online and other studies criticized app ability to deliver promised benefits.

In addition, data protection authorities and investors could require additional documentation in case of data breaches or due diligence processes.

WHAT DIGITAL HEALTH COMPANIES NEED TO DO ENSURE COMPLIANCE WITH GDPR?

Most of the GDPR requirements apply to Digital Health companies in the same way as they do for other types of business (eCommerce, Finance etc). However, **these are some of the requirements which are more challenging for developers**.

THE CONSENT

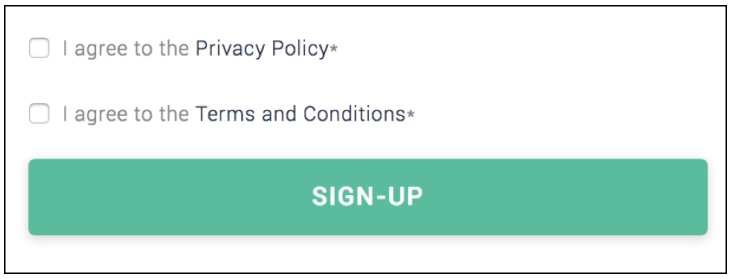
According to the GDPR, the processing of health data is prohibited unless you comply with one of the six methods or grounds for processing such data. The most common method for getting the permission for processing health data is the "**explicit consent**", which is typically implemented via checkboxes on websites or apps during signup process.

Companies must pay extreme attention on this and implement methods to obtain a valid consent. A valid consent is the one that is freely given, specific, informed, granular, explicit indication of the data subject's agreement for the processing of her personal data.

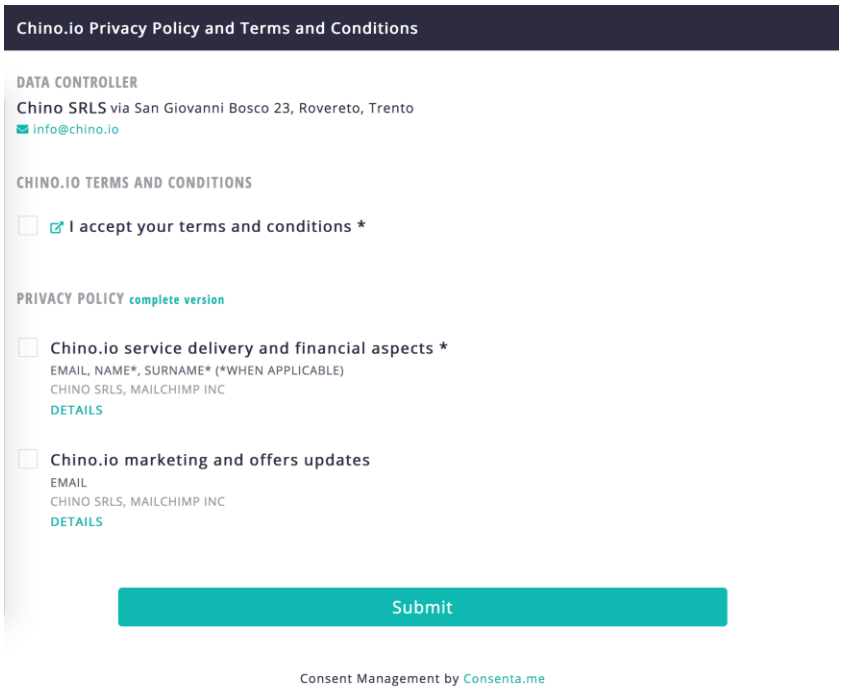
So obviously the following consent screenshot – from an Italian website - is **not a valid consent** (and it wasn't even with the old Directive).

The following screenshot is much better, but it's still not valid since:

+ it's not granular since you must accept all policy terms to use that service (even marketing)
+ it's not informed since you need to click on the policy link and read legalese terminology to understand what's going to happen with your data.



According to best practices, the consent form should be structured as follows and must contain all information about data processors (in addition to granular choices and other requirements).



In addition to showing properly the information, developers must provide a proof that data subjects have given their consent lawfully. This means that developers must keep record of consents, updates, withdrawals, and be able to demonstrate their compliance if required by the supervisory authority.

THE DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The DPIA is a document that demonstrates that you have completed a risk assessment and identified the necessary measures to comply with GDPR dispositions and demonstrate that your businesses do not represent high risk for users.

By following a risk-based approach and by analyzing the nature, scope, context, and purpose of your processing, you will be able to show how risky is your activity and potential impacts on data protection and, more generally, on the rights and freedoms of EU citizens.

The main source that provides a brief and official guideline about the DPIA is the Art 29 Working Party Guidelines (also contained in folder “DPIA-Data Protection Impact Assessment”). The art 29 WP defines the

requirements for the DPIA (since not all companies need to do it) and how to perform it. Therefore, check that document and consult specialists to understand if you need to do a DPIA.

Therefore, check in the Art 29 WP document if you need to do the DPIA. If you do, then carrying out a DPIA which must be based on your business specific risks. The DPIA can be carried out by any person/organization inside or outside the business if explicitly appointed by you.

DATA PROTECTION OFFICER (DPO)

The DPO is a new professional figure introduced by GDPR and who responsible for the direction and overseeing of all data protection activities within a company. The appointment of a DPO is mandatory if:

- the core activities of the processing require regular and systematic monitoring of data subjects on a large scale;
- the core activities of the company involve processing on a large scale of special categories of data e.g. health (Art. 9 GDPR).

Some of the tasks of DPO are:

- Conduct privacy training; inform and advise the controller or the processor and the employees on Privacy Matter; Identify ongoing privacy compliance requirements, e.g., law, case law, codes, etc.
- Provide advice where requested on the DPIA and monitor its performance pursuant to Article 35; Maintain DPIA guidelines and templates.
- Maintain records of the transfer mechanism used for cross-border data flows (e.g., standard contractual clauses, binding corporate rules, approvals from regulators).

As a health business which process health sensitive data you may need to appoint a DPO. Further guidelines could be provided by the most recent interpretations on this aspect, which consider the size of the company and other aspects. Therefore, check the guidelines or contact (more than one) lawyer for the latest interpretations.

TECHNICAL AND SECURITY MEASURES

The **implementation of technical and security requirements has been always the most important** and also the most challenging aspect to demonstrate compliance with the old Directive and the new GDPR.

Health applications in particular require highest possible security due to the sensitivity of managed data and complexity of the sector. Some of the principles and tips to start with are:

+ Privacy and Security by Design and by Default
+ Encryption
+ Pseudonymization

Privacy and Security by Design principles are system engineering approaches which take privacy and security into account throughout the entire development of a project, service or product (Art. 25(1) of GDPR).

Privacy and Security by Design mandates to developers the "implementation of appropriate technical and organizational measures" (e.g. **pseudonymization and encryption**) in an effective manner "at the time of the determination of the means for processing and at the time of the processing itself". The final aim is to "implement data-protection principles" from the very beginning of the design of a project, service or product.

Privacy by Default is identified by art. 25(2) GDPR, which requires the same technical and organizational measures to be applied "for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" (also known as **data minimization**).

Pseudonymization & Encryption are techniques that developers **must implement** to protect health data, and to reduce the potential harm in case of data breaches. Encryption is the best strategy in terms of security and legal responsibility since **encrypted data are not private data** and therefore losing encrypted data means no fines and no notifications are needed.

However, encrypted data are not searchable and therefore developers must find alternatives and complex compromises. One of such compromises is pseudonymization, which (if implemented properly), can reduce drastically risks for users. The most typical approach to pseudonymiziation (also mandated by the Italian Data Protection law) is the separation between personal identifiers and health records.

ASSESSMENT OF YOUR SERVICE PROVIDER'S CONTRACT (e.g. CLOUD PLATFORMS)

Frequently, startups implement their health applications using cloud-based services and platforms which are not suitable for healthcare. Some most common mistake examples are Google Firebase or Heroku, which can be very useful for standard apps, but that do not provide sufficient guarantees for health data management and (X)applications.

Important contract aspects that developers must check:

- that the service provider is HIPAA compliant, in other terms if it provides sufficient guarantees for healthcare applications in US. Even though HIPAA is not a EU law, this is a reliable benchmark to assess if developers can use a US based product also in the EU. Firebase and standard Heroku offering are not HIPAA compliant. Note that, even though Google Cloud Platform, Amazon AWS and other IaaS providers are HIPAA compliant, they still have to implement technical aspects as: record level (or application level) encryption, access control, authentication, GDPR requirements like right to be forgotten etc.
- that the service provider ensures guarantees about data location. While all cloud providers nowadays provide such guarantees, platforms like Firebase don't do that. In this case relying on Privacy Shield (old Safe Harbour) agreements could be a risky choice given the widespread fear of health data being sent outside EU.
- that the service provider gives you explicit guarantees about privacy and data security. It is the developers' responsibility to choose properly the service provider. If this does not provide clear definitions of its responsibilities for sensitive data management, then it should be a very important warning.

OTHER RELEVANT REGULATIONS

It's important to notice that GDPR provides only high-level framework and a **starting point** for Digital Health developers. Namely, GDPR provide definitions of users' rights and developers' obligations, while the technical implementations of such requirements is delegated to security best practices, system administrators and some guidelines defined by more technical bodies (Art 29 Working Party, ENISA), international security standards (NIST, ISO 270XX), and Member States laws (French HDS Agreement, German Guidelines for Health Applications). Note that **Member States laws are still valid under GDPR**, and will have the power to introduce additional restrictions, which provide additional barriers for developers.

RESOURCES

- https://www.dataprotection.ie/docs/10-09-14-Global-Privacy-Sweep-raises-concerns-about-mobile- apps/1456.htm
- http://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-015-0444-y

- http://ec.europa.eu/justice/data-protection/reform/index_en.htm

@chino_api
@zidia

Jovan Stevovic

Jovan Stevovic, CEO and co-founder of **Chino.io**. He holds a PhD in Computer Science at the University of Trento, Italy. He founded Chino.io in 2014 after spending 5 years in R&D department at the GPI Spa, a large company working in healthcare sector in Italy and working on development of health services considering privacy, security and regulatory compliance requirements.
With Chino.io he won different prizes at EU level has been selected as one of most promising Digital Health / Cyber Security startups by the EU Commission (prizes and Seals of Excellence)
Chino.io helps 50+ digital health companies in the EU to solve security and compliance challenges by offering them its secure Database as a Service and API health data.

Author: Jovan Stevovic, Chino.io CEO and co-founder.