FUTURE INTERNET
SOCIAL TECHNOLOGICAL ALIGNMENT in HEALTHCARE

www.fi-star.eu
www.fistarblog.com
@fistarproject
www.facebook.com/fistarproject

Legal compliance for developers using FI-STAR eHealth platform

Training materials

(prepared by Tilburg University)

Target audience and objectives

- **Target audience**:
  - developers & other potential users of the FI-STAR eHealth platform as a service (PaaS)
- **Objective**:
  - the audience will become familiar with and be able to recognise and understand legal issues of the field of eHealth generally and specifically when an eHealth PaaS is involved.
  - They will be able to anticipate on these issues when developing their respective apps, and able to effectively communicate to their expert legal advisors about these issues

Disclaimer

- These training materials are based on the European Union law
- No part of these training materials constitutes legal advice.
- To ensure legal compliance, the developers should work closely with a legal expert competent to advice on matters of law applicable in countries where the respective eHealth solutions will be implemented.

Outline

1. Introduction: eHealth platform as a service and legal landscape of eHealth *(Part I)*
2. Privacy and data protection: legal issues and compliance strategies *(Part II)*
3. Safety and performance requirements: legal issues and compliance strategies *(Part III)*

Part I:
Introduction
eHealth PaaS and legal landscape of eHealth

Legal landscape of mHealth solutions

- Requirements with **direct impact** on design:
  - Safety and performance requirements
  - Data protection
- **Not regulated on EU level**: definition of a medical professional, liability of medical professionals, etc.

- Requirements with **no direct impact** on design:
  - Rules on electronic commerce *(information rights and guarantees in the context of distance and online contracts)*
  - Rules on patients' rights in cross-border healthcare

Important characteristics of mHealth

- Intended contexts of use and functionalities;
- Cloud-based;
- Modular architecture;
- Multi-sourced

Contexts of mHealth

- **Consumer apps**
  - lifestyle and wellbeing apps such as FitBit; diet diaries; meditation apps; sleep apps, etc.

- **Apps intended for healthcare context**
  - health services provided by **health professionals** to **patients** to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices (Art 3 Patients' Rights Directive in the context of *cross-border healthcare)*

Cloud-based

- "Cloud computing consists of a set of technologies and service models that focus on the *Internet-based use and delivery of IT applications, processing capability, storage and memory space*."

(Article 29 Working Party opinion WP196)

Modular architecture

- **Modular** architecture, new functionalities by combining pre-existing elements:
  - Smart devices (phones, tablets)
  - Sensors (blood-glucose meter)
  - Mobile computers

  (Thuemmler et al 2013)

Multisourced architecture

- **Multisourced** architecture:
  - Each component can be provided by a different party

Part II

Data protection:

legal issues and compliance strategies

What is ‘data protection’ (‘DP’)?

- *Privacy* protects **information relating to ‘personal life’,** not all information about a person;
- *Data protection* covers **all information** relating to a person who is identified or can be identified;
- Data protection is not the same *as (medical) confidentiality;*
- Data protection law regulates if, when, and under what conditions ‘personal data’ can be processed, and gives an individual rights to control information about him/herself.

General principles of DP

Article 6 (1): Personal data must be:

(a) processed **fairly** and **lawfully;**

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. **[purpose specification & purpose limitation]**

(c) adequate, relevant and not excessive in relation to the purposes**; [proportionality]**

(d) accurate and, where necessary, kept up to date**; [data quality]**

(e) Kept in identifiable form for no longer than is necessary for the purposes […] **[data minimization]**

See FI-STAR Checklist for DP compliance for a detailed, eHealth specific explanation of each principle

The key concepts

What is ‘personal data’? (1/4)

- **’Personal data’** is “any information relating to an identified or identifiable natural person ('data subject'); an *identifiable* person is one who can be identified*, directly or indirectly*, in particular by reference to an *identification number* or to … factors specific to his physical, physiological, mental, economic, cultural or social identity.” (Art 2(a))

What is 'personal data'? (2/4)

- Any information
- Relating to a data subject:
  - Directly or indirectly (e.g. through an object that belongs to the individual, e.g. value of a house) (WP136)
- Identified or identifiable [natural person]:
  - directly (e.g. by name) or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.)"
  - by all means "reasonably likely to be used", taking technological development into account
- "Either by the controller or by any other person to identify the said person." (Recital 26 + WP136)

What is ‘personal data’? (3/4)

- "**Anonymous** data" (WP 136, 216)
  - any information relating to a natural person
  - where the person cannot be identified by the data controller or by any other person,
  - taking account of all the means likely reasonably to be used by any person to identify that individual.
  - Data protection does not apply to truly and irreversibly anonymized data (Recital 26)
  - Anonymisation is an instance of data processing in itself
- **Pseudonymisation** is masking of personal data that allows re-identification (see Reform definition in Art 4(2a))
  - Directive: Personal data → still subject to data protection
  - Reform: Lighter compliance burden (“[…] processing limited to pseudonymous data should be presumed to meet the reasonable expectations of the data subject based on his or her relationship with the controller. ” (Recital 38 Regulation proposal)

FI-STAR Aid

- FI-STAR developed a decision tree ‘Does your product, process or service process ‘personal data’
- FI-STAR eHealth PaaS platform users to whom UK law applies may use this *UK ICO decision tree* that the UK supervisory authority suggests

What is 'health data'?

No definition in 1995 **Directive:**

- 'data concerning health';
- **'Special category'** of personal data with **a higher standard of protection** (Art 8)
- Processing **is prohibited**, unless an exception applies.

Examples (in a WP Letter of 2015)

- Medical data
- Broader range of data on the health status (membershship in groups: AA, WeightWatchers)
- Disease risk (raw data over a period of time)
- Grey areas (← technological developments, e.g. FB status)

Definition in the Proposed **reform**:

- any personal data which relates to the physical or mental health of an individual, or to the provision of health services to the individual (Art 4(12))

Examples (Recital 26):

- the registration for the provision of health services; payments or eligibility for healthcare; a number, symbol or particular assigned to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services; biological samples, etc.

FI-STAR aid: what is health data?

- To decide if your app involves processing of health data *see FI-STAR decision-tree "Does your app process health data"*

Who is responsible?

- **'data subject**' is an identified or identifiable natural person; *(Art 2(a))*
- **'controller'** is the natural or legal person, … which alone or jointly with others determines the purposes and means of the processing of personal data; *(Art 2(d))*
  - Bears data protection obligations (Art 6(2)) and liability (Art 23)
  - Defined *pragmatically* (WP 169): factual rather than only formal ability to determine means and goals of processing
  - Multiple controllers possible (WP 169)
- '**processor**' is a natural or legal person, … which processes personal data on behalf of the controller; *(Art 2(e))*
  - *Bears contractual responsibility to controller, not the data subject*

Who is responsible? Problem cases

- whether an app provider is a controller in relation to data that an ***app user*** disclosed himself and agreed top terms of use; and
- the division of responsibility between the app providers and ***third parties***: operation systems, infrastructure, platforms and devices on which the eCoaching apps are run.

Lawful processing of health data - Art 8 -

1. Member States shall **prohibit … the processing** of data concerning health … .
2. Paragraph 1 shall not apply where:

(a) **explicit consent** […], except where prohibited by laws of the Member State; or

(b) necessary for the purposes of carrying out the obligations and rights of the controller in the field of **employment law** […]; or

(c) necessary to protect the **vital interests** of the data subject or of another person where the data subject is […] **incapable of giving his consent**; or

(d) processing is carried out […] by a **non-profit-seeking body** […] and relates solely to its members or to persons who have regular contact with it […]; or

(e) Data are **manifestly made public** by the data subject or for the establishment, exercise or defence of **legal claims**.

3. […] required for **the purposes of preventive medicine, medical diagnosis, the provision of care or treatment** or the management of health-care services, and where those data are processed by a **health professional** subject […] to **the obligation of professional secrecy […]**

Data subject's explicit consent
- Art 8 (2)(a) -

Consent must be an "*indication of [the data subject's] wishes* by which the data subject signifies his agreement to personal data relating to him being processed" (Article 2(h)).

- ***Explicit*** (WP 131):
  - No 'opt-out';
  - explicitly relate to the sensitive nature of health data, demonstrate that the data subject is aware that he renounces the special protection of health data.
  - **Consent to undergo a certain medical treatment does not equate "explicit consent"**
- ***Freely given***
  - Expression of a genuine choice (WP 131)
- ***Specific***
  - relates to a well-defined, particular situation & purpose. A 'general agreement' to the processing does not constitute specific consent (WP 131)
- ***Informed***
  - based on an understanding of the processing event(s) and their possible implications, as well as of the consequences of refusing consent

Context of treatment relationship
- Art 8 (3) -

- Purpose:
  - preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services,
- Processed by a health professional or by another person:
  - within the limits of the treatment contract, “the direct bilateral relationship between a patient and the health care professional/health care institution consulted by the patient.” (WP 131)
- Subject to the obligation of professional secrecy (or equivalent):
  - Effective sanctions (WP 131)

FI-STAR aid

- For detailed explanation of how data protection principles, rights and obligations apply in the context of health apps see *Checklist "Data Protection Compliance"*

What is PIA?

- Privacy cannot be assessed by a snap-shot evaluation (e.g. fitness) – 'privacy by design' is next best thing
- PIA is a process and *"method to both ensure and ascertain that the product, service or process does not present or effectively mitigates data privacy risks"*
- Privacy is likely to be safeguarded when a PIA process/method is fully and effectively implemented

The PIA elements

- Throughout technology development & implement-n, as early as possible
- Identified privacy ***risks***
- Privacy ***targets***
- Risk-***mitigating*** measures
- Identification of ***responsible*** parties
- PIA ***procedures*** (ε stakeholder consultations, documentation)
- ***Re-assessment***: periodic and if changes were made (the feedback loop)

FI-STAR aid

- See privacy / data protection impact assessment ('DPIA') flowchart

Part III
Safety and performance of eHealth apps

EU safety & performance

- Only **safe** products can be placed on the EU market;
- What is safe?
- How do we establish that technology is safe?

What is safe?

- **General legislation**
  - *Product Safety Directive* (Directive 2001/95/EC of 3 December 2001 on general product safety) 'GPSD'
  - Applies to manufactured *products*
  - When/to the extent *the specific legislation is insufficient or absent* (Art 1(2) GPSD)

- **Specific legislation** (Medical Device Framework)
  - Directive 90/385/EEC on active implantable medical devices,
  - Directive 93/42/EEC on medical devices (MDD), and
  - 98/79/EC of the European Parliament and of the Council on in vitro diagnostic medical devices.

Product – definition (Art 2(a)(b) GPSD)

- **Product**

  "***any product*** — including in the context of providing a service — which is ***intended for consumers*** or ***likely*****,** under reasonably foreseeable conditions, ***to be used by consumers*** even if not intended for them, and is supplied or made available […] in the course of a ***commercial activity***, and whether new, used or reconditioned."

- **Safe product**

  "under normal or reasonably foreseeable conditions of use […] ***does not present any risk*** or only the ***minimum risks*** […], considered to be acceptable and consistent with a high level of protection for the ***safety and health of persons***"

Medical device - definition (Art 1(2)(a)MDD)

"any instrument, apparatus, appliance, ***software***, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application,

intended by the manufacturer to be used for human beings

for the purpose of:

(a) diagnosis, prevention, monitoring, treatment or alleviation of disease, **(b)** diagnosis, monitoring, treatment, alleviation or of compensation for an injury or handicap, **(c)** investigation, replacement or modification of the anatomy or of a physiological process, **(d)** control of conception

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means."

Key points

- **No safety & performance requirements apply to some eHealth apps:**
  - **Not clear** if software is a product:
    - Def of a product *does not mention* software;
    - Not clear if / how apps pose a *risk to health* (Staff Working Doc)
  - **Subjective definition** of a medical device; Intent to be established by 'the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional materials.' *Art 1(2)(g) of MDD*
  - **No binding EU rules** on distinguishing between lifestyle/wellbeing apps and apps that are medical devices;

Commission Guidelines (January 2012)

- ***Non-binding***;
- Explains by way of ***example***
  - Software is likely not a MDD:
    - Performs "storage, archival, compression, communication or simple search";
  - Software is likely a MDD:
    - Used "for the evaluation of patient data to support or influence the medical care provided to that patient";
    - Generates alarms;
    - decision-support systems "which combine medical knowledge databases and algorithms with patient specific data […] to provide healthcare professionals and/or users with recommendations"

Aids to help determine if your app is a MDD

- If your medical app is a medical device, safety and performance requirements apply,
- Check this simple and clear European Commission guidance document on Qualification and Classification of stand alone software with a decision tree and this infographic.

What is safe?

- An eHealth app is safe when it meets the ***generic essential safety and performance requirements*** (i.e. apply to all medical software;
  - apply depending on the device's intended purpose.
  - listed in Annex I MDD.

- ***Compliance is presumed*** when applications are in conformity with the relevant national ***standards*** adopted pursuant to the harmonized European standards (Art. 5(1) MDD);
  - developed by 'competent organisations' based on state of the art of technology;
  - ***Voluntary*** compliance with standards.

(Selected) Essential requirements

- The devices must ***not compromise the clinical condition or the safety*** of patients, or the safety and health of users (s.1);
- The devices must perform as intended (s.3);
- Specific to the ***intended purpose*** of the app, e.g. alarm function; measuring and display function, etc.
- If the device is intended for use ***in combination*** with other devices or equipment, ***the whole combination*** […] ***must be safe*** […].(s.9.1).
- "the ***software*** must ***be validated according to the state of the art*** taking into account the principles of development lifecycle, risk management, validation and verification" (s.12.1.a) – to ensure stability and repeated performance of software
- ***Risk*** management (s.2):
  - eliminate or reduce risks as far as possible,
  - take adequate protection measures […] in relation to risks that cannot be eliminated,
  - inform users of the residual risks due to any shortcomings of the protection measures adopted.

Who assesses safety?

- The '**manufacturer'**
  - "the natural or legal person ***with responsibility*** for the design, manufacture, packaging and labelling of a device before it is **placed on the market under his own name**, regardless of whether these operations are carried out by that person himself or on his behalf by a third party" (Article 1(2)(f) MDD); 'manufacturer' ≠ 'producer'
- The **'notified bodies'** – **private bodies with a public function**
  - bodies designated by the Member States to perform conformity assessment (Article 16 MDD). The list of the notified bodies, their identification numbers and "the tasks for which they have been notified", is published and kept up-to-date by the Commission in the Official Journal of the European Communities. the manufacturer may apply to **a notified body of his choice** within the tasks for which that body is notified (Article 11(9) MDD).
- The **'competent authorities'**
  - the national authorities of the Member States. They are endowed with supervisory functions regarding the notified bodies.

Assessment procedures

IN ORDER TO GET MARKET ADMISSION

- **Class I** (low risk) – most of apps - Assessment carried out by the manufacturer;
- **Class IIa** - the intervention of a notified body is compulsory at the *production* stage;
- **Classes IIb, III** (high risk) - inspection by a notified body is required with regard to the *design and manufacture* of the devices;
- **Class III** (highest risk) - ***explicit prior authorization of the notified body*** with regard to conformity before the device is placed on the market.

→ **CE MARK** (Art 17 MDD) ascertains not the compliance with essential requirements, but that the device ***has gone through the conformity assessment procedure***

TO REMOVE FROM THE MARKET

- Vigilance and marker surveillance by the manufacturer;
- Competent authorities record and evaluate incidents, inform the Commission (Art 10 MDD)
- Liability claims (outside the scope of MDD)

Other requirements

- For the legal requirements for clinical investigation of new medical devices see *Checklist on legal compliance when new medical apps are developed and tested*