ACONTRARIO

DEEP LEARNING = DEEP LIABILITIES

The (potential) legal and ethical challenges in digital health

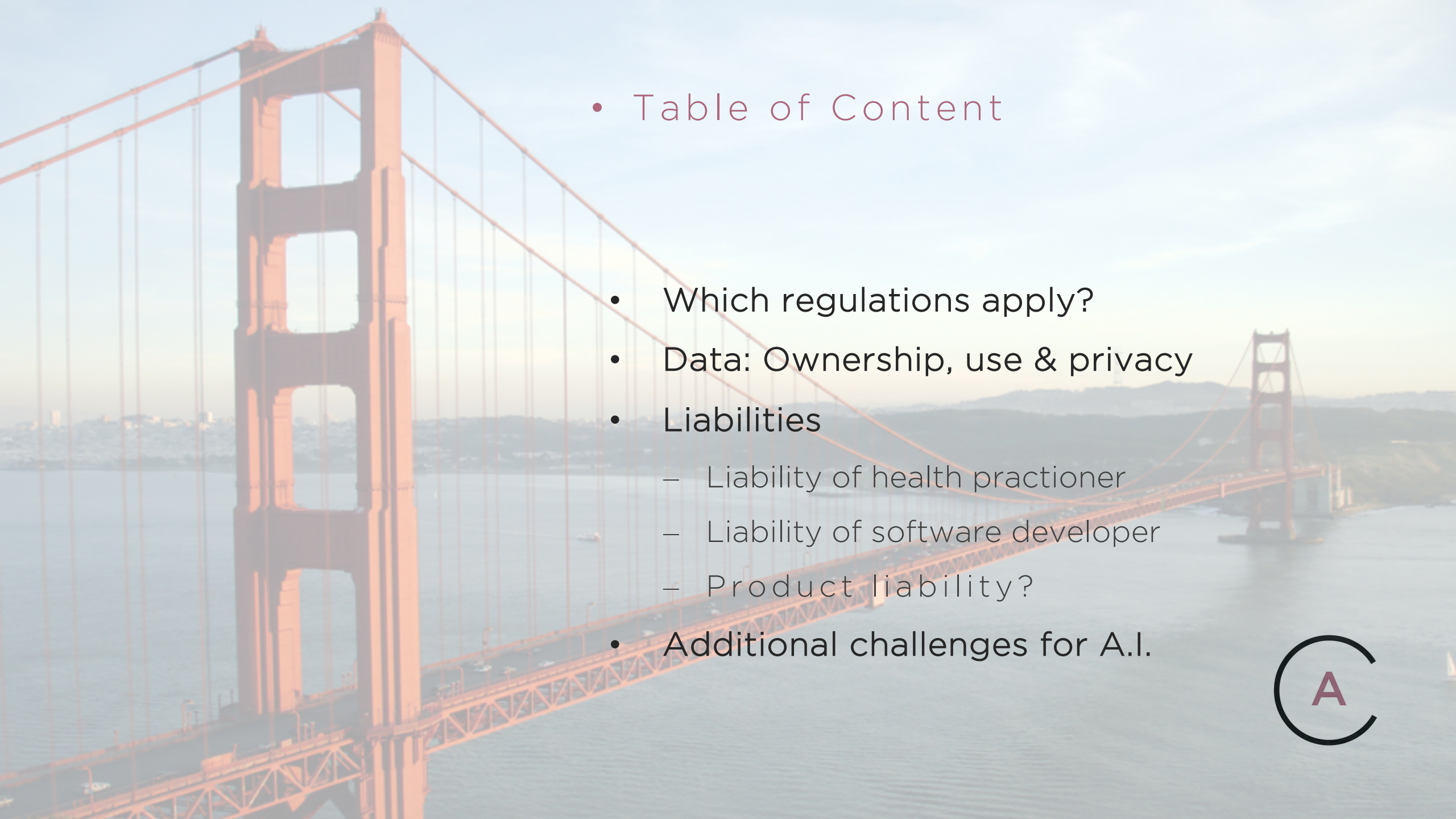


Table of Content

- Which regulations apply?
- Data: Ownership, use & privacy
- Liabilities
  - Liability of health practioner
  - Liability of software developer
  - Product liability?
- Additional challenges for A.I.

- Chapter I

- Which regulations apply?

- Which regulations apply?

- Intended use of the software components (or sum of components)?
  - Medical device? CE Marking?
  - Drug-device combination product

- Which regulations apply?

  - Medical device? CE Marking?

  - Remark

Definition ‘medical device’ Art. 2.1 EU-Regulation 2017/745 (1)

- any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:
  - diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
  - diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
  - investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
  - providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

Definition ‘medical device’ Art. 2.1 EU- Regulation 2017/745 (2)

- The following products shall also be deemed to be medical devices:
  - devices for the control or support of conception;
  - products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point.

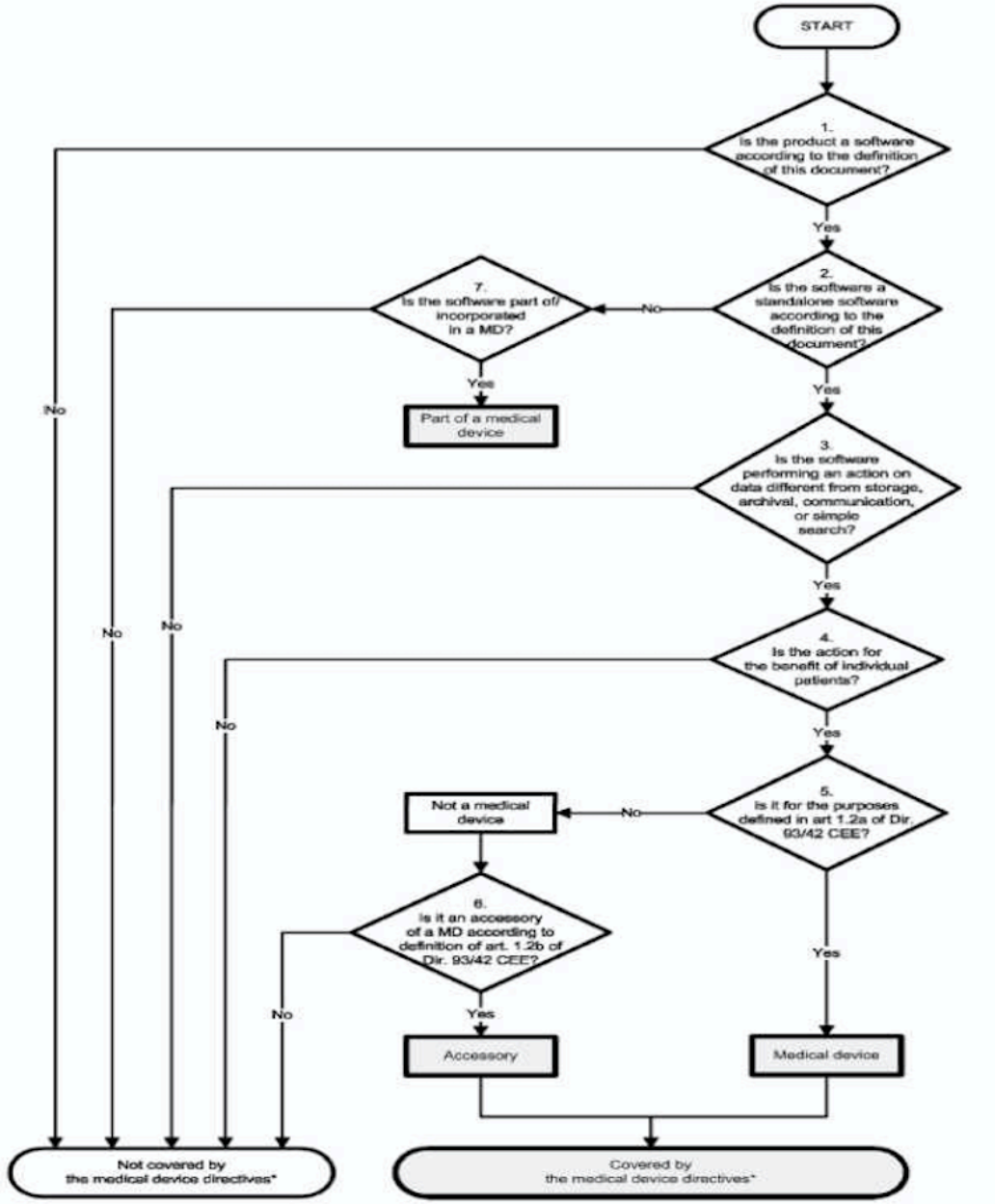


Figure 1: A decision diagram to assist qualification of software as medical device.

- Which regulations apply?

  - Medical device? CE Marking?

  - Remark

- Which regulations apply?

- What kind of claims can you make about your digital health solution?
  - Pharmaceutical companies:

  = digital health solution impacts the marketing of your drugs
    - FDA, EMA, China's CFDA or SAIC
    - Regarding the advertising, promotion or labeling

- Which regulations apply?
  - USA:
    - Solution = medical device
      - Advertising and labeling will be subject to FDA or FTC regulation
  - EU:
    - no harmonized regulation on labeling and advertising
  - China: therapeutic claims
    - China's drug and/or device regulation
    - Advertisement Law
    - CFDA pre-approve all adverts

- Data: ownership, use and privacy

- Best Practice:

  Identify jurisdiction that you operate in or offer your services, and those that present the highest risk to your company. Then assess what data you collect and the purposes for which you use it to identify which specific laws and regulations apply

• Chapter II

- Data: Ownership, Use & privacy

- Data: ownership, use and privacy

- Ownership of data?
- Ownership of outcome? Methodologies? (predictive) models?
  - IP Rights
    - Patents, trade secrets, copyrights, database rights

- Data: ownership, use and privacy

- Ownership of data?
  - Imperative to implement a decent IP-strategy
  - Contractual framework with
    - Collaborative partners
    - Employees and independent contractors
    - Suppliers
    - clients
    - support services (SLA)

- Data: ownership, use and privacy

- Competition authorities:
  - Data that:
    - cannot be replaced
    - Is necessary for the development of new products
    - Will not quickly become outdated
  - => may be required to provide access to third parties

- Data: ownership, use and privacy
- Data Protection

- Data: ownership, use and privacy

- Data Protection – GDPR

- Advantages of GDPR
  - Harmonisation
  - Make it an USP
  - Data centralisation, clear data mapping

- Data: ownership, use and privacy

- 10 steps to GDPR-compliancy
  1. Processing? Of Personal Data?
  2. Legal ground?
  3. Basic principles
  4. Data subject rights
  5. Technical and organizational measures
  6. Data protection by design and by default
  7. Create Awareness
  8. DPO
  9. Data Breach notification
  10. Relationship DC ⇔ DP

- Data: ownership, use and privacy
- 10 steps to GDPR-compliancy

1. Processing? Of Personal Data?
    - Challenge in Health Care:
        - anonimized data
        - Medical data = special categories
2. Legal Ground
    - Exemption for treatment
    - Consent?
        - Solution:
            - Primary use
            - Secondary use

- Data: ownership, use and privacy
- 10 steps to GDPR-compliancy
  3. Basic principles
     - Data minimalisation
     - Purpose limitation
       - Big data?
       - AI?
       - Blockchain?

  Solution by EU

  - Principles as data minimalisation and purpose limitation
    - not absolute
    - To be interpreted in light of purpose of processing

- Data: ownership, use and privacy

- 10 steps to GDPR-compliancy
  4. Data subject rights
  - Right to be forgotten
  - Challenges in healthcare
    - Medical legislation > GDPR
    - Not the same as right to delete
    - = putting out of use

- Data: ownership, use and privacy

- 10 steps to GDPR-compliancy

5. Technical and organizational measures
6. Data protection by design and by default

- Challenges for developers!
- Innovation = data protection by design

- Data: ownership, use and privacy

- 10 steps to GDPR-compliancy

  10. Relationship DC ⇔ DP

  DC ⇔ DP = DPA

  DC ⇔ DC = DSA

  Ownership is not the same as quality re GDPR

- Data: ownership, use and privacy

Data Protection

- USA
  - HIPAA
  - State medical privacy laws in California and Texas
- China
  - Medical Institution Records Administrative rules + Administrative Measures for Population Health Information

- Data: ownership, use and privacy

- Use of Data
  - No limits on data use:
    + progress is quicker,
    + care more efficient
    + health benefits
    - No confidence re purpose
    - Discrimination
    - Higher insurance costs
    - Overall: might lead not to seek medical help

- Data: ownership, use and privacy

- Use of Data
  - Placing excessive restrictions on patient data:
    + confidence re use
    +. No discrimination
    - No efficiency
    - Timely treatment??
    - Too many administrative boundaries to provide effective treatment
    - Overall: might prevent treatment altogehter

- Data: ownership, use and privacy

- Use of Data: Healthcare professionals should respect the following three key principles of health information:
    1. Individuals have a fundamental right to privacy and confidentiality of their health info
    2. Individuals have a right to control access to and disclosure of their health information by giving, withholding or withdrawing consent
    3. For any non-consensual disclosure of confidential information HPs must have regard to its necessity, proportionality and attendant risks

- Data: ownership, use and privacy
- Use of Data

  - Solution
    - Primarily use
      - Patient's Interests:
        - first and foremost: effective and efficient delivery of care
    - Secondarily use
      - Patient's Interests:
        - Greater concerns about how their health data is bing used, with whom it is shared...

- Data: ownership, use and privacy
- Use of Data

  - Solution
    - Primarily use
      - Medical legislation
      - Provisions of GDPR
    - Secondarily use
      - Provisions in GDPR
      - Support new ethical framework on health data and data donation

- Data: ownership, use and privacy
- Use of Data
  - Focus points:
    - sufficiently secure storage, appropriate purposes, secure confidentiality, compliance and accountability obligations
    - For secondary use:
      - permitted purposes, necessary safeguards, location and platform

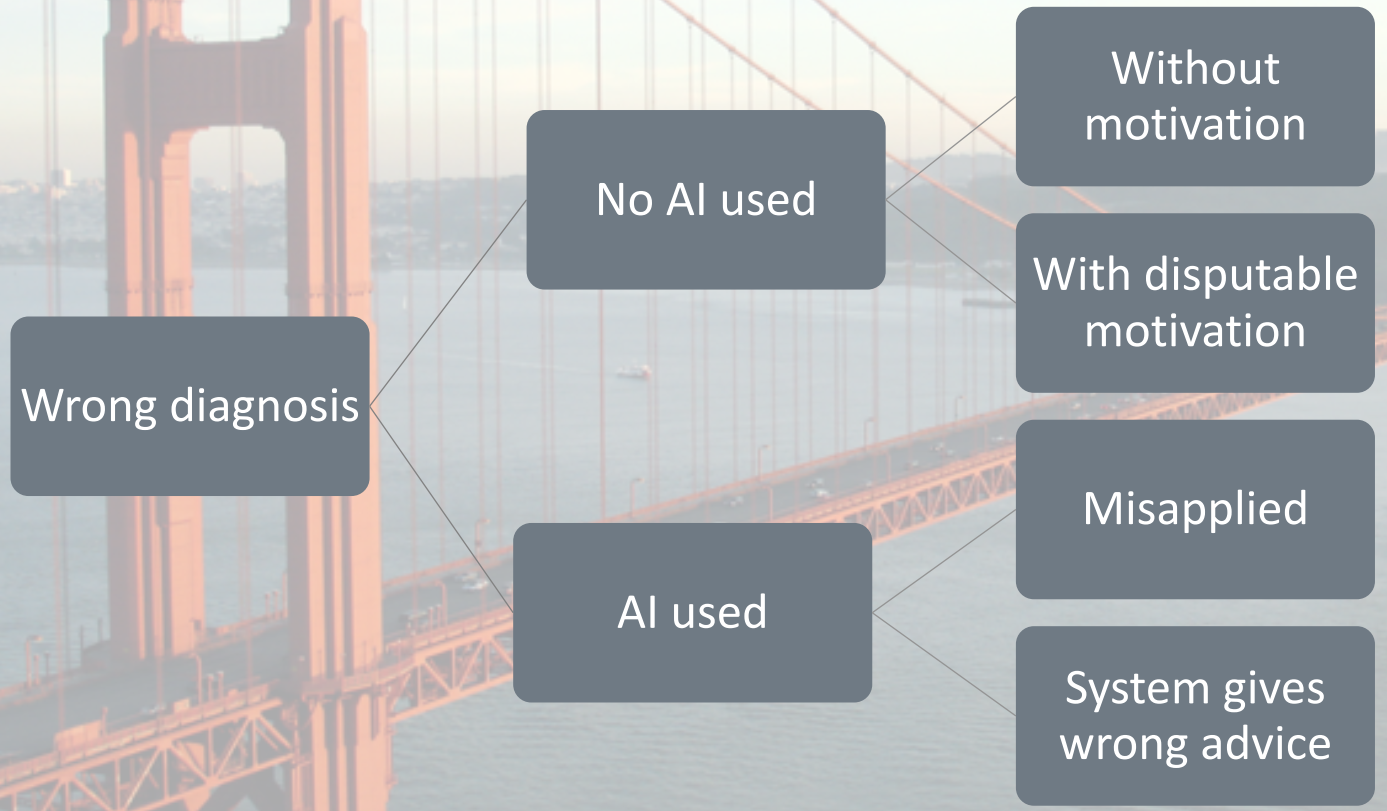
• Chapter III

- Liabilities
  - Liability of health practioner
  - Liability of software developer
  - Product liability?

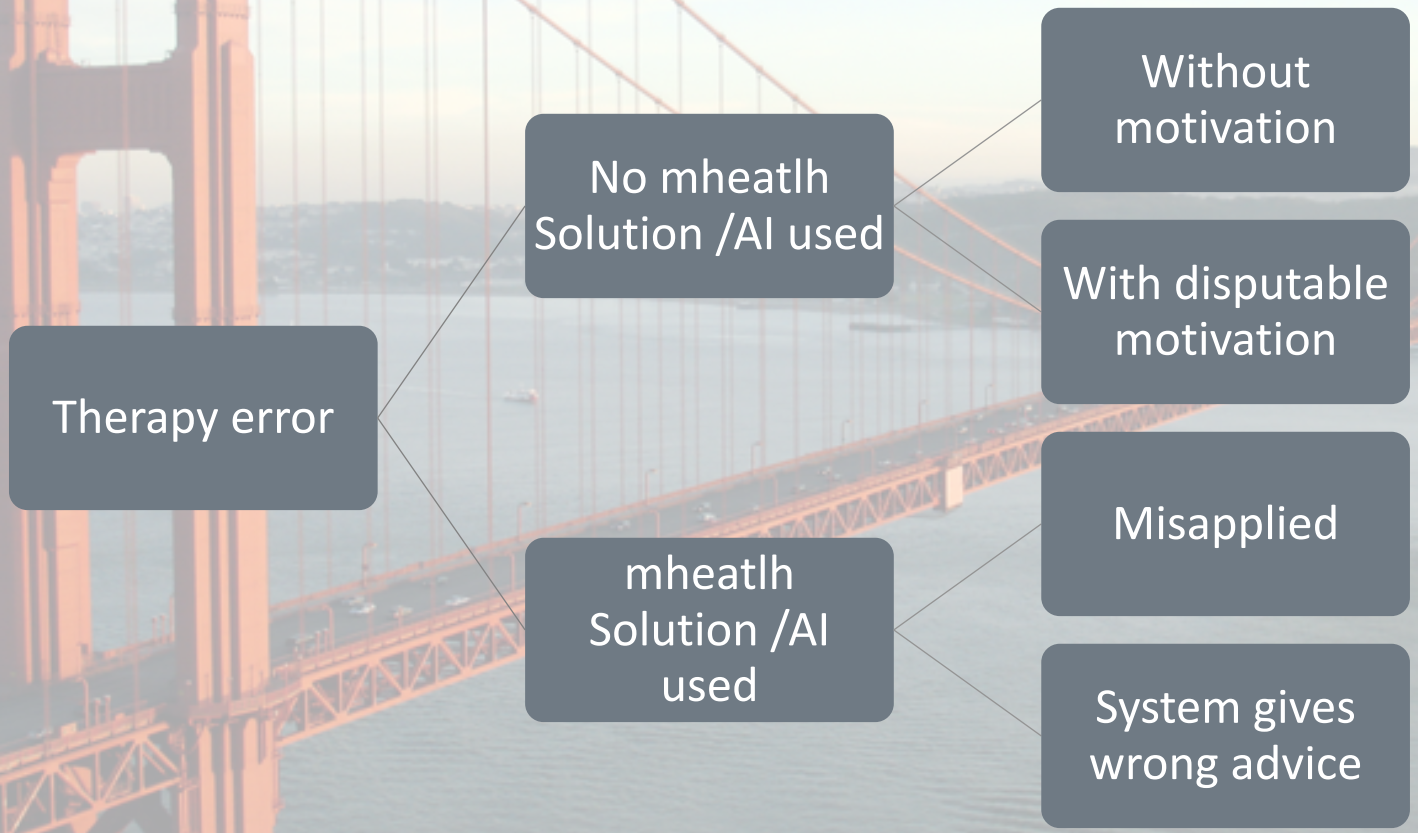
- What are possible claims? And against who?

- Basis of possible claims

- Basis of possible claims



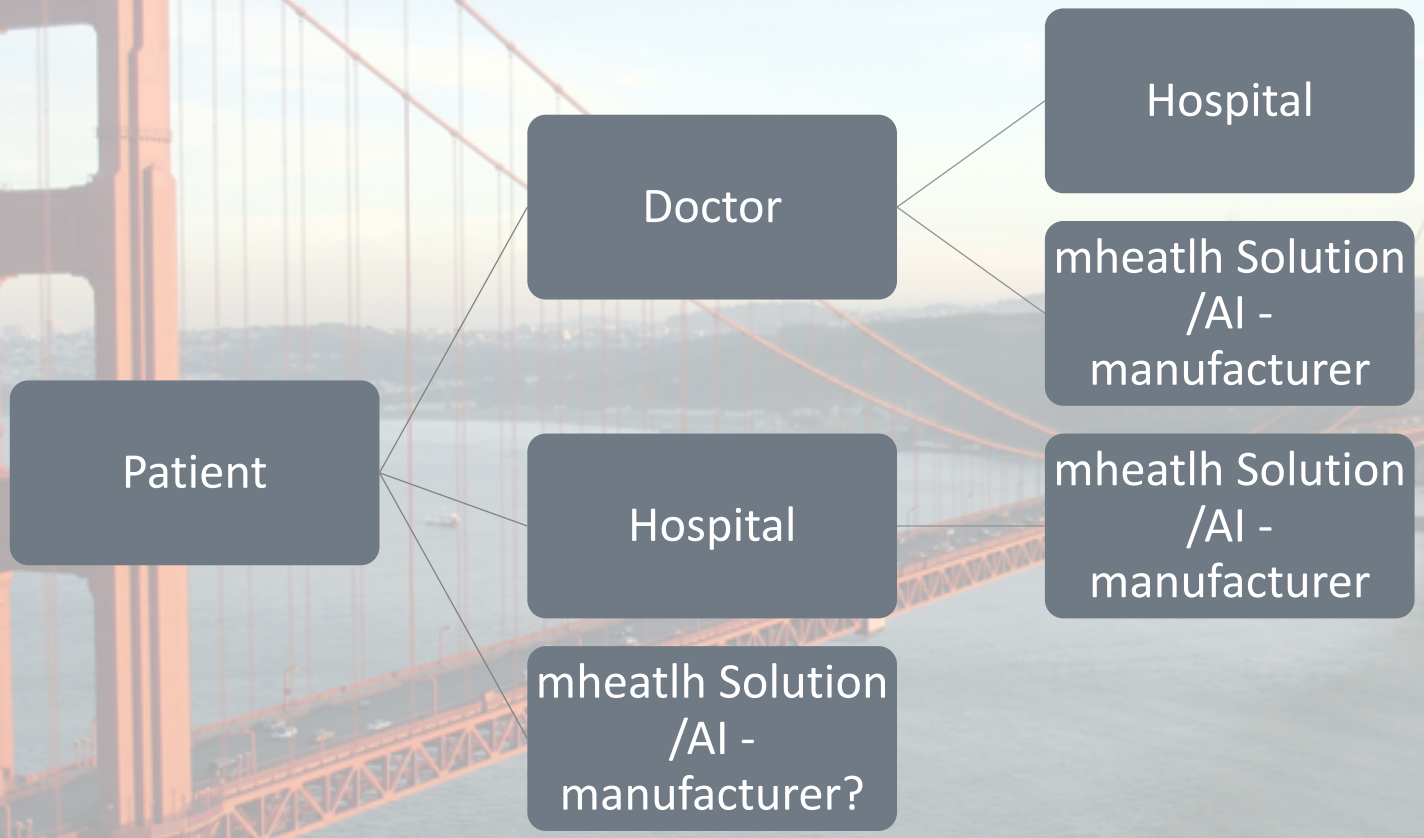
- Basis of possible claims



Against who?

- Patient decides on
  - Procedure (civil or criminal)
  - Whether or not via the Medical Accident Fund
  - Parties to the main proceedings (in civil proceedings)
  - Legal basis
    - Contractual, extra-contractual or product liability
    - Pleas in law
- Doctor or hospital can claim indemnification against manufacturer of the AI-system

- Against who: Schedule



- Liability against hospital/physician: How will claims against physician or hospital be assessed?

- In the case of both contractual and extra-contractual liability, the claimant must always prove three elements
  - Fault/Misconduct
  - Damages
  - Causality between fault and damages => causal link

Liability against hospital/physician:

- Fault is assessed according to “general care” criterion (or 'culpa levis in abstracto’- criterion)

- Concrete behaviour must always be compared with the (hypothetical) figure of the
  - Normal, careful doctor (‘bonus medicus’)
  - Of the same category
  - Placed in the same external conditions

Liability against hospital/physician: The Bonus Medicus

- Educates himself
- Follows the current state of science
- Carries out (or has carried out) the necessary technical examinations
- ‘Provides only health care for which he has the necessary proven competence and experience’ (art. 8 Quality Legislation)
- Refers when necessary
- Follows (validated) guidelines (or can justify why he does not do so)
- Ensures the safety of the equipment and tools he uses (or has it done)

- Liability against hospital/physician: No use of mHealth application/ AI

- Failure to use AI systems with proven benefits
  - may constitute professional negligence

- Not using AI will have to be justified

Liability against hospital/physician: Use of AI

- Diagnostic and therapeutic decision-making needs to be globally motivated
  - AI is ‘clinical decision support’
  - Testing of all elements of the case to professional standard remains possible and necessary

Liability against hospital/physician: Use of AI

- Does security obligation include evaluation of the reliability of the AI system?
  - Is this possible?
    - By an individual doctor?
    - By a service or an hospital?
  - Does regulation on medical devices help?

Liability against hospital/physician: Use of AI

- Claims (in indemnity) against AI manufacturer are certainly possible on the basis of contractual liability, but great discussion is not unthinkable about:
  - Exact purpose of AI
  - Exact extent of the commitment
  - Disclaimers

• Liability against App/AI developer

- Tort Law
  - Art. 1382 Civil Code:
    - Fault/misconduct – damages – causal link
    - Misconduct is an act by a human being (?)
    - not always possible
  - Art. 1383 Civil Code
    - No misconduct but negligence and imprudence

Liability against App/AI developer

- Tort Law
  - Art. 1384 Civil Code
    - Liable for damages caused by a person for whom one is responsible
  - Art. 1384, 1st Civil Code
    - Objects under custody
  - Art. 1384, 3rd Civil Code
    - Damages caused by servants

Liability against App/AI developer

- Tort Law
  - Art. 1385 Civil Code
    - Damages caused by animal under its custody
  - Product liability
    - Act of 25/02/1991
    - Issue: Tangible movable asset

• Chapter IV

- Additional challenges for A.I.

- Define Artificial Intelligence

- A good definition is important for the assessment of the ethical challenges

• Define Artificial Intelligence

Classic scientific definition:

- AI is
  - a growing resource of interactive, autonomous, self-learning agency
  - which enables computational artifacts to perform tasks that otherwise would require human intelligence
  - to be executed successfully.

(A.L. Samuel, 1960)

Ethical & Legal challenges

- AI is data driven

- How to obtain and how to govern your data
  - Consent (China?)
  - Ownership
    - medical data
      - Patient or mHealth developer
  - Privacy/Data Protection
    - Who has access
    - Purpose
    - Right to be forgotten
  - Secure storing

• Ethical & Legal challenges of A.I.

- AI needs more & more data (but good selection of training data!)

⇔

- Ethics & Legal: less data (data minimisation)

- What are the possible implications of artificial intelligence for professional liability?

  - Possibly significant steps forward in quality and safety
  - Possibly fewer diagnostic errors
  - Possibly better supporting therapeutic decisions
  - The end of defensive medicine' (Shailin Thomas, Harvard blog)

But also great worries

- Risk of wrong conclusions (correlation is not necessarily causality!)
- Insufficient attention to individual complexity
  - Multi- morbidity
  - Drug interaction
  - Social-psychological determinants
- ‘Black box’: ‘opacity' of decision-making
- Insufficient independence in determining the algorithm
  - Depending on techno giants
  - Possible (occult) commercial influence

- Ethical & legal challenges

- New ethical & legal challenges

1. Lack of transparancy & predictability
2. Potentially harmful?
    - Intentional vs. Unintentional
    - Responsibility & liability
3. Erosion of human self-determination

Ethical challenge 1: Lack of transparancy & predictability

- Why need for transparant & predictable algorithms
  - Computer says NO
  - Legal system is build on predictability
- Whitebox vs. blackbox algorithms

E.C. 1: Transparency & Explainability: blackbox algorithms

Challenges:

- IP rights?
- Starting point:
  - not enough emphasis/focus on:
    - selection of TRAINING DATA
- Accuracy
  - Technical challenge
    - Initiatives: IBM & DARPA (see later)

- E.C. 2 AI potentially harmful?

a force for good!

- Lower diagnostic errors by 85% in breast cancer patients
- Reduce time to identify and neutralize cyberattacks from 101 days to a few hours

a force for Evil/bad

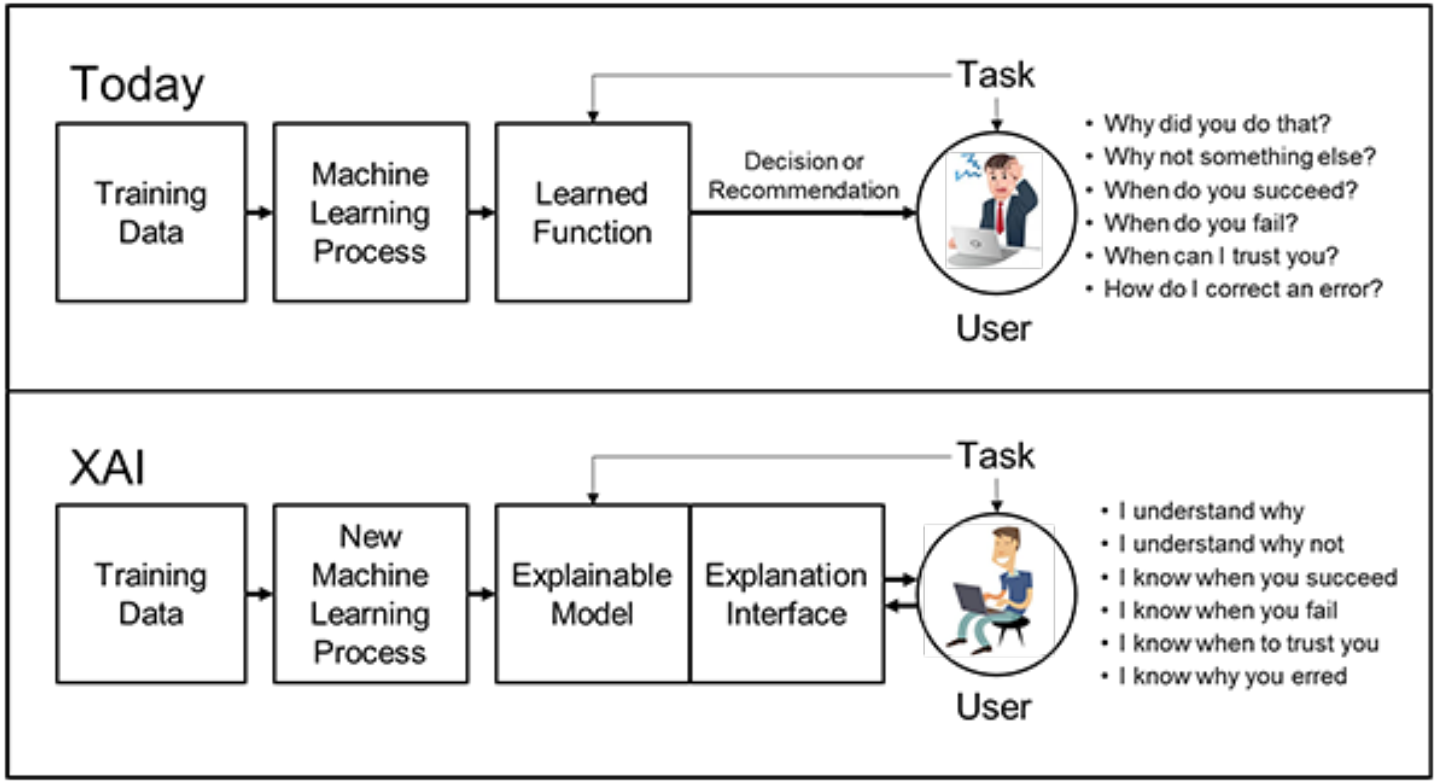
- Intentional
- Unintentional
  - COMPAS

E.C.2 - Intentional vs. Unintenial harm

- Ethics code: Hippocratic Oath - Do no harm!
- Ethical training
- Techniques to explain AI and predict the outcome
  - Don’t go too far
    - Hungry judges syndrome
  - IBM & DARPA

E.C.2 - Solutions

- Techniques
  - DARPA



E.C. 2: Responsibility & liability

- Distributed agency:
  - Developers, designers, users and software and hardware
- Faultless responsibility regime
  - Good practices for delegation
  - Ethical code

E.C. 3 - Erosion of human self-determination

- Ethical analyses
  - Invisible influence by AI on human behaviour
- Defined set of ethical principles
  - Yet ethics depend heavenly on cultural and social context + region
    - IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems

- Comparative analysis

- Once identified

- → translate into reliable guidelines to shape AI-based innovation

Initiatives

- From corporate:
  - AI4People
- From government:
  - EU Commission: High Level Expert Group
  - China? Social score system

Identifying ethical risks

- Formulation of methodologies
  - testing
  - Impact assessment analyses
    - Step by step evaluation of impact of technologies on aspects such as transparency, privacy & liability

ACONTRARIO

Magali Feys - AContrario

Founder – IP, IT & Data Protection Lawyer

A: Huize Minne – Kortrijksesteenweg 62
B – 9830 Sint –Martens- Latem

E: magali@acontrario.law

M: +32 474 29 61 25

W: www.acontrario.law