# WS2: Legal and regulatory frameworks for health data

Pirkko Nykänen

Tampere university

4.8.2021

# Starting principle

- **Health-related personal data is confidential and sensitive and it has to be protected for non-authorised access, use and disclose**
- Laws, normative rules, guidelines and standards define the framework for data access, processing and disclose

# EU – GDPR: GENERAL DATA PROTECTION REGULATION, effective from May 2018

- **Purpose - Harmonize privacy and data protection laws across Europe**
  - **to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business**
  - GDPR was driven by the concern that individuals' personal information was being exploited in ways that undermined privacy and, by extension, democracy

- **Digital economy should operate with the informed consent of users and clear rules for companies who seek to do business in the European Union**
- https://gdpr.eu/what-is-gdpr/

- **GDPR** states that
- processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited

  - GDPR allows that special categories of data, such as **health data, may be processed for necessary archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**

    - The scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research

-

- General Data Protection Regulation (GDPR) binds organizations to strict new rules about using and securing they collect from people, including the mandatory use of like encryption and higher legal thresholds to justify data
  - Anonymization of data is necessary, truly anonymized data cannot be linked back to an individual -- pseudonymized data must be treated as personal data, therefore consent is needed
  - GDPR will levy harsh fines against those who violate its privacy standards, with penalties reaching into the tens of millions of

- **With GDPR Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence**

# Data processing, data subject, data controller and processor

- **Data processing** — Any action performed on data, whether automated or manual, e.g. collecting, recording, structuring, storing, using, erasing… so basically anything
- **Data subject** — The person whose data is processed
- **Data controller** — The person who decides why and how personal data will be processed
- **Data processor** — A third party that processes personal data on behalf of a data controller
  - The GDPR has special rules for these individuals and include cloud servers

# GDPR data protection principles

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified
4. **Accuracy** — You must keep personal data accurate and up to date
5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using
7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles

# It is allowed to process personal data - when

- The data subject gives you **specific, unambiguous, informed consent** to process the data
- Processing is necessary to execute/enter into a contract to which the data subject is a party
- You need to process it **to comply with a legal obligation**
- You need to process the data **to save somebody's life**
- Processing is necessary **to perform a task in the public interest** or to carry out some official function
- You have a **legitimate interest** to process someone's personal data
  - This is the most flexible lawful basis, though the "fundamental rights and freedoms of the data subject" always override your interests, especially if it's a child's data

# Informed consent

There are strict rules on the **consent from a data subject** to process his/her information

- **Consent must be "freely given, specific, informed and unambiguous"**
- **Requests for consent must be "clearly distinguishable from the other matters" and matters" and presented in "clear and plain language"**
- **Data subjects can withdraw previously given consent whenever they want, and you want, and you have to honor their decision**
  - **You can't simply change the legal basis of the processing to one of the other justifications justifications**
- **Children under 13 can only give consent with permission from their parent parent**
- **You need to keep documentary evidence of consent**

# Persons' privacy rights

GDPR recognizes **privacy rights for data subjects**, which aim to give individuals more control over the data they loan to organizations, and as an organization, it's important to understand these rights to ensure you are GDPR compliant

1. **The right to be informed**
2. **The right of access**
3. **The right to rectification**
4. **The right to erasure**
5. **The right to restrict processing**
6. **The right to data portability**
7. **The right to object**
8. **Rights in relation to automated decision making and profiling**

# GDPR applies to you even when you're not in the EU

- *1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of **a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not***
- *2. This Regulation applies to the processing of personal data of **data subjects who are in the Union by a controller or processor not established in the Union**, where the processing activities are related to:*
  - *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
  - *(b) the monitoring of their behaviour as far as their behaviour takes place within the Union*
- *3. This Regulation applies to the processing of personal data by **a controller not established in the Union, but in a place where Member State law applies by virtue of public international law***

# Major data protection regulations in Finland

# Personal Data Act, 523/1999

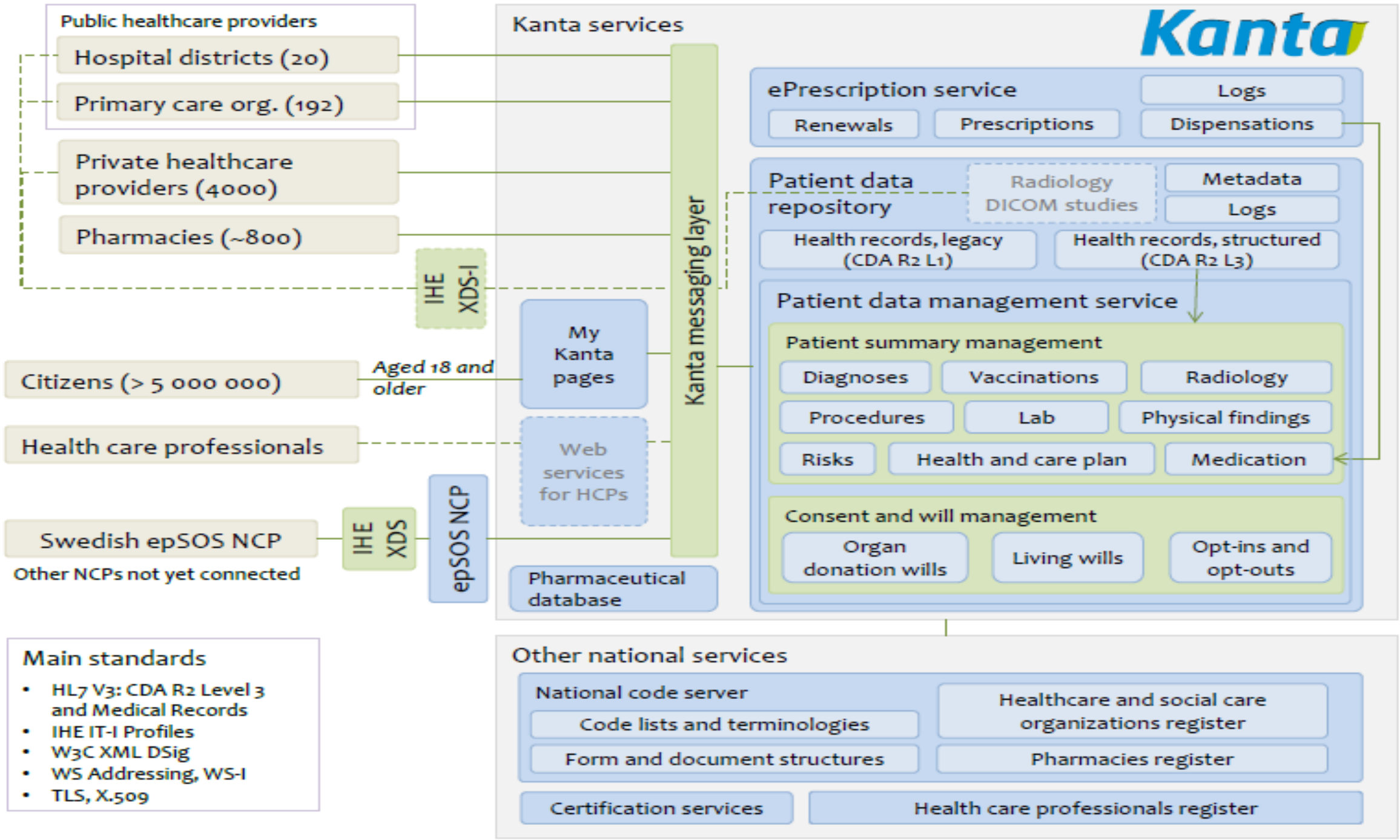
- General rules for collection, storage, usage, exchange and disclose of personal data
- **Important  requirement is to define the purpose why personal data is collected and processed**
- General principles for personal data management:
  - Pre-planning, responsibility to protect
  - Good practice in data processing and management
  - Purpose of use has to be respected
  - Necessity to process, realiability requirement
- **Personal data builds a personal data register, the one who collects is responsible for collection, storage, reliability, access and disclose**
- Physical and organisational data protection has to be organised
  - Data security and protection organisation and responsbilities have to be defined

# Act on personal data management in social and health care, 159/2007

- Improves the possibilities to use ICT in social and health care
- Enables patient data access when and where needed
- Promotes information access for patients and citizens
- Archiving of digital patient documents
  - Central national archive – eArchive
  - Consent management
  - Permanent storage of patient documentation
  - Patient documents are transferred/accessed by local and regional health information systems and by citizens

# Act on health care services, 1326/2010

- Concerns health care functionalities, tasks and health care services
- Gives a citizen the possibility to select the service providers, across community boundaries
- Purpose is to strenghen primary care services, promotion of health and welfare and access to health services and their efficient provision
- Focuses also on good customership and collaboration between primary care and specialised care
- **All registers inside a hospital district form a federated patient data register**
  - **No consent is needed inside the region, but the patient has still a right to deny the disclose of his/her data inside the region**


Public healthcare providers
Hospital districts (20)
Primary care org. (192)
Private healthcare providers (4000)
Pharmacies (~800)
IHE XDS-I
Citizens (> 5 000 000)
Aged 18 and older
Health care professionals
Swedish epSOS NCP
Other NCPs not yet connected
IHE XDS
epSOS NCP
Kanta services
Kanta
My Kanta pages
Web services for HCPs
Pharmaceutical database
Kanta messaging layer
ePrescription service
Logs
Renewals
Prescriptions
Dispensations
Patient data repository
Radiology DICOM studies
Metadata
Logs
Health records, legacy (CDA R2 L1)
Health records, structured (CDA R2 L3)
Patient data management service
Patient summary management
Diagnoses
Vaccinations
Radiology
Procedures
Lab
Physical findings
Risks
Health and care plan
Medication
Consent and will management
Organ donation wills
Living wills
Opt-ins and opt-outs
Other national services
National code server
Code lists and terminologies
Form and document structures
Healthcare and social care organizations register
Pharmacies register
Certification services
Health care professionals register
Main standards
HL7 V3: CDA R2 Level 3 and Medical Records
IHE IT-I Profiles
W3C XML DSig
WS Addressing, WS-I
TLS, X.509

# Data protection in Tanzania

- **Electronic and Postal Communications Act** (EPOCA), 2010:
  - EPOCA guards against the violation of any person's entitlement to respect and protection of person, the privacy of their own person, their family and matrimonial life, and respect and protection of their residence and private communications
- **Tanzanian Cybercrimes Act, 2015**
  - allows law enforcement to search and seize computer systems, data, and information without a court order, eroding the constitutional right to privacy, and it also permits the police to use invasive surveillance methods such as keylogging devices or software that records keystrokes in real time, without judicial authorisation or oversight
- https://dataprotection.africa/tanzania/

- **DATA PROTECTION SITUATION IN TANZANIA? National legal framework? Specific regulation for privacy ?**

# Thank you for your attention!

Pirkko.Nykanen@tuni.fi