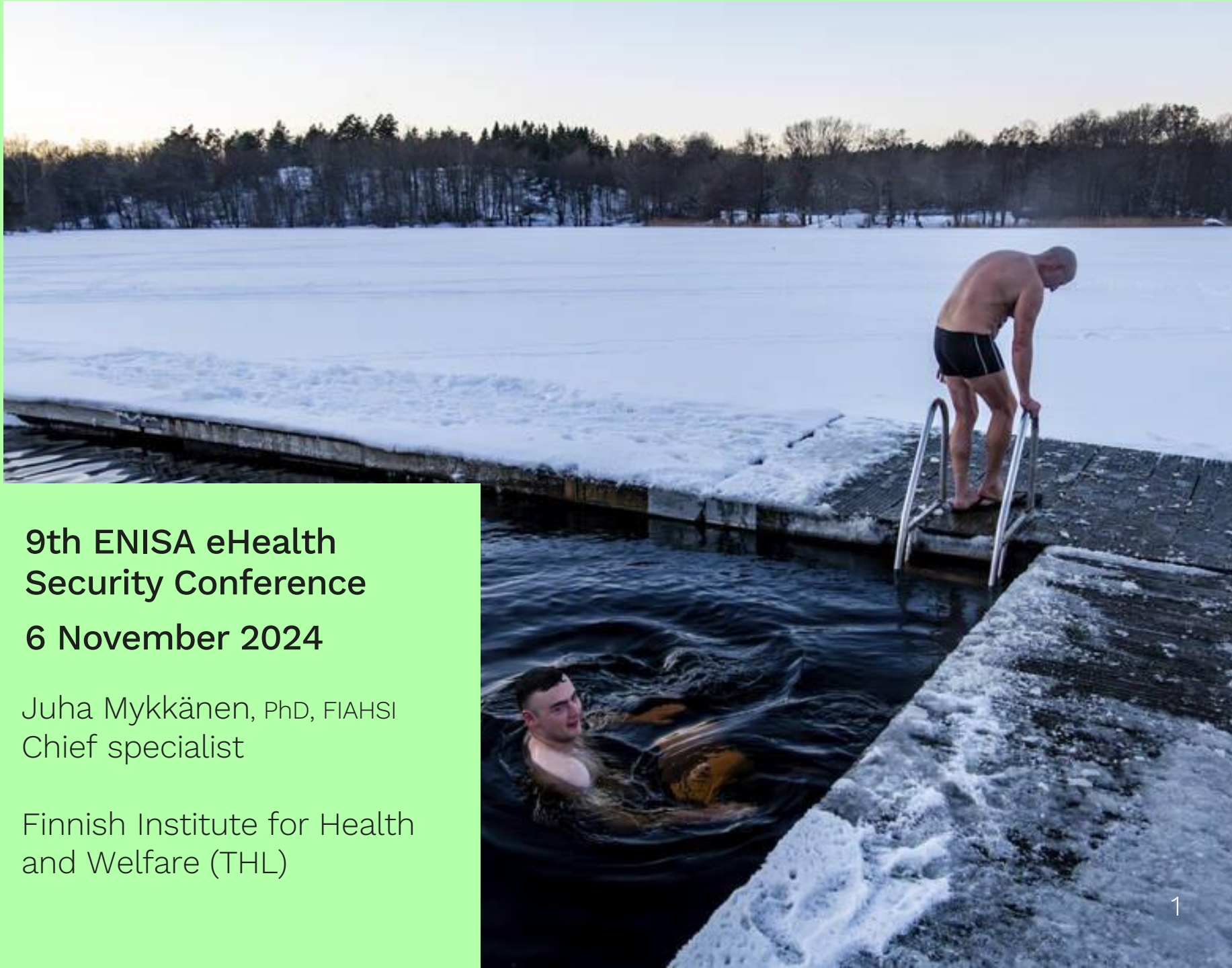


National and European security requirements in health data sharing – case Finland

9th ENISA eHealth Security Conference

6 November 2024

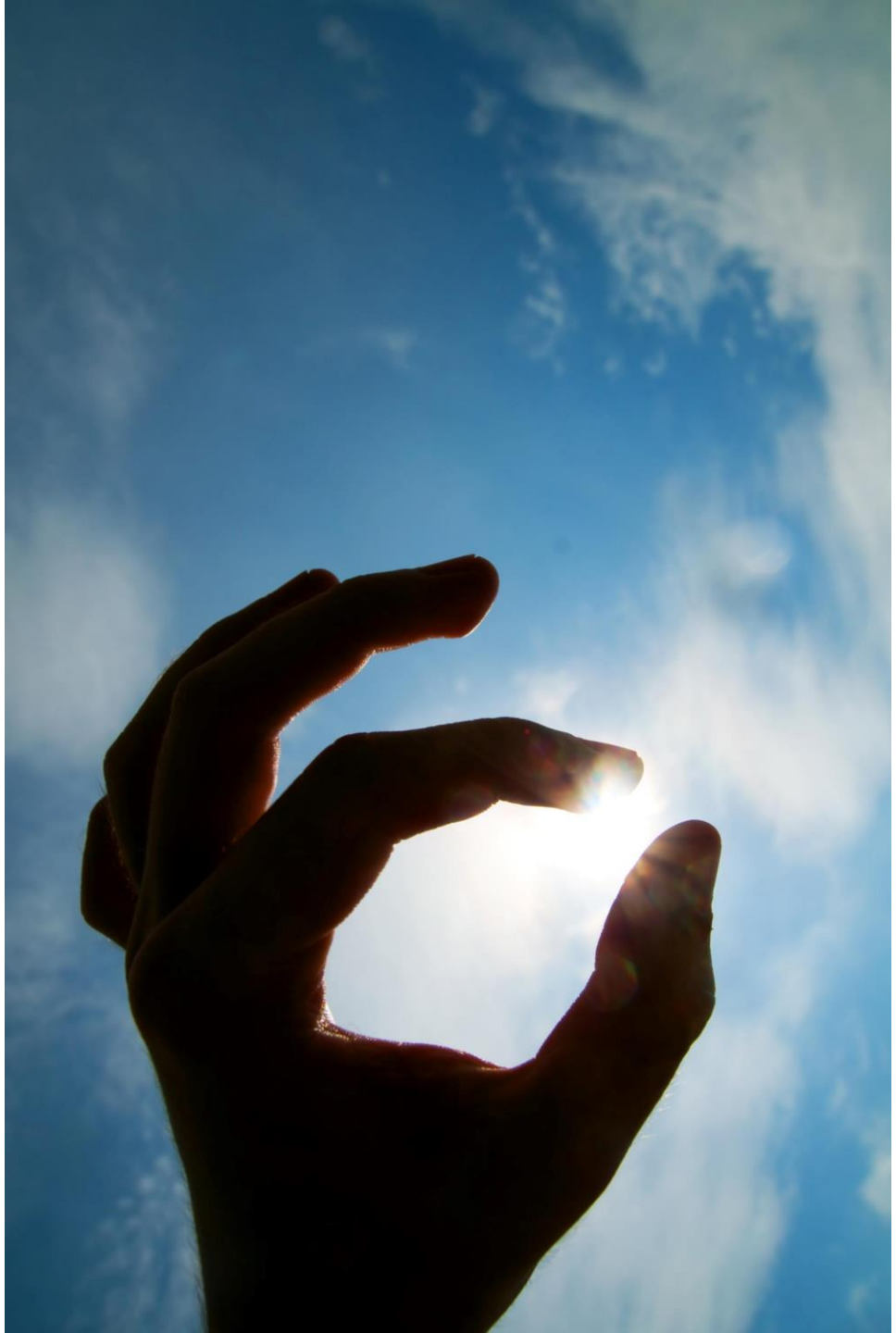
Juha Mykkänen, PhD, FIAHSI
Chief specialist

Finnish Institute for Health and Welfare (THL)

Funded by the European Union

Contents

- Background and context
- Regulatory framework and governance
- Essential requirements and certification
- Reflections and European viewpoints
- Summary



Background and context

Social and health care information management in Finland - context

- Long-standing national strategies (1996-, 2007-, 2014-, 2023-) and legislation (2000, 2003, 2007, 2014, 2021, 2023) to support the use of IT for health and social services
- Current law for client data processing, selected key points
  - Roles for national agencies
  - Mandatory use of **national health IT infrastructure** (pharmacies, public and private health and social service providers)
  - **Registration** of information systems for health and social services
  - **Certification** of interoperability and security (most central systems – class A)
- In addition to legislation, informational and funding steering: enterprise architecture, national development programmes, many different collaboration groups and forums
- Wellbeing services counties (n=21) in health and social services reform (2023) in very different situation in relation to main information systems in health and social services

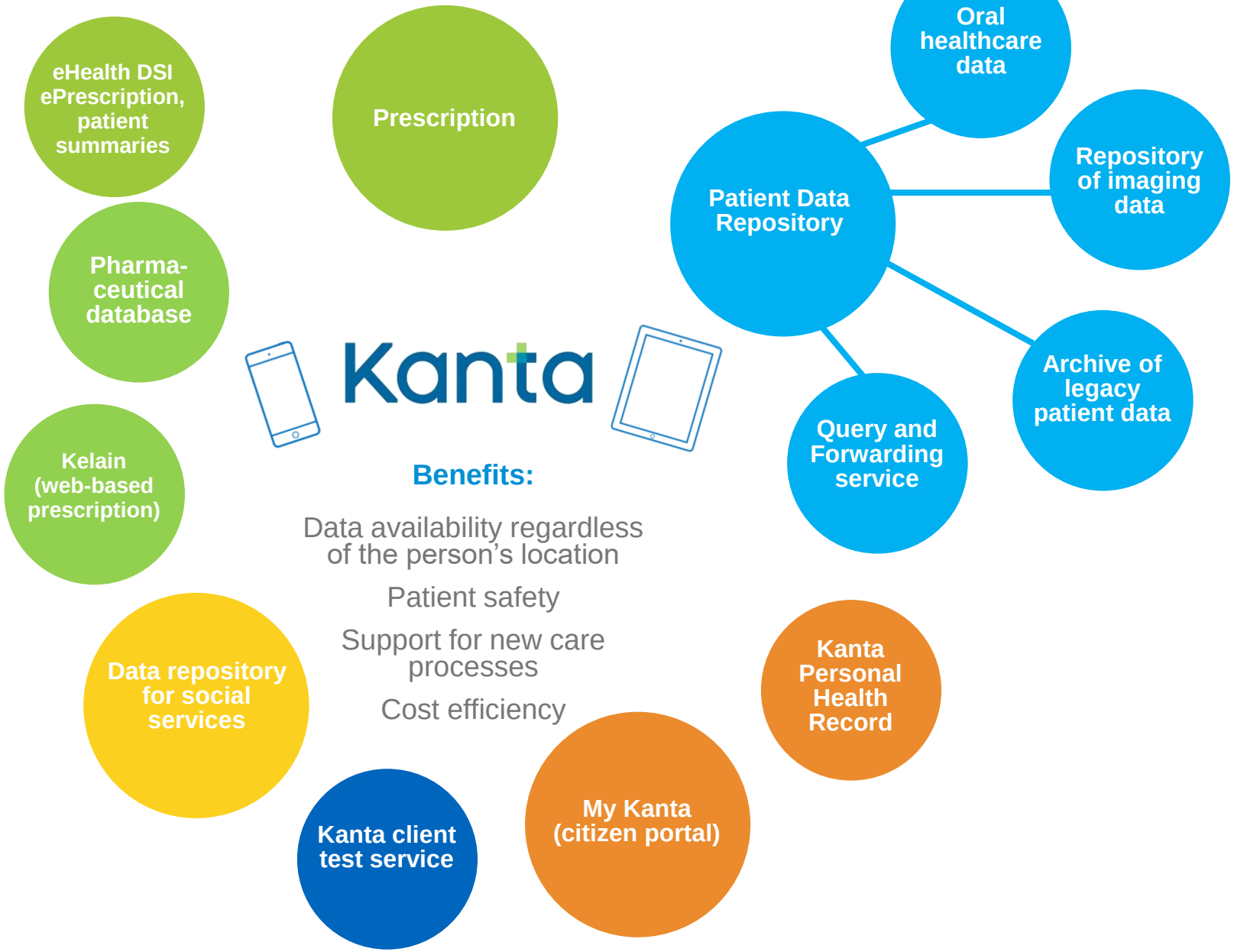
National Infrastructure in Finland: Kanta

Type: **Centralized**

Coverage: **National**

Operational since: **2010 (ePrescriptions)**

Use: **through local systems and portals**



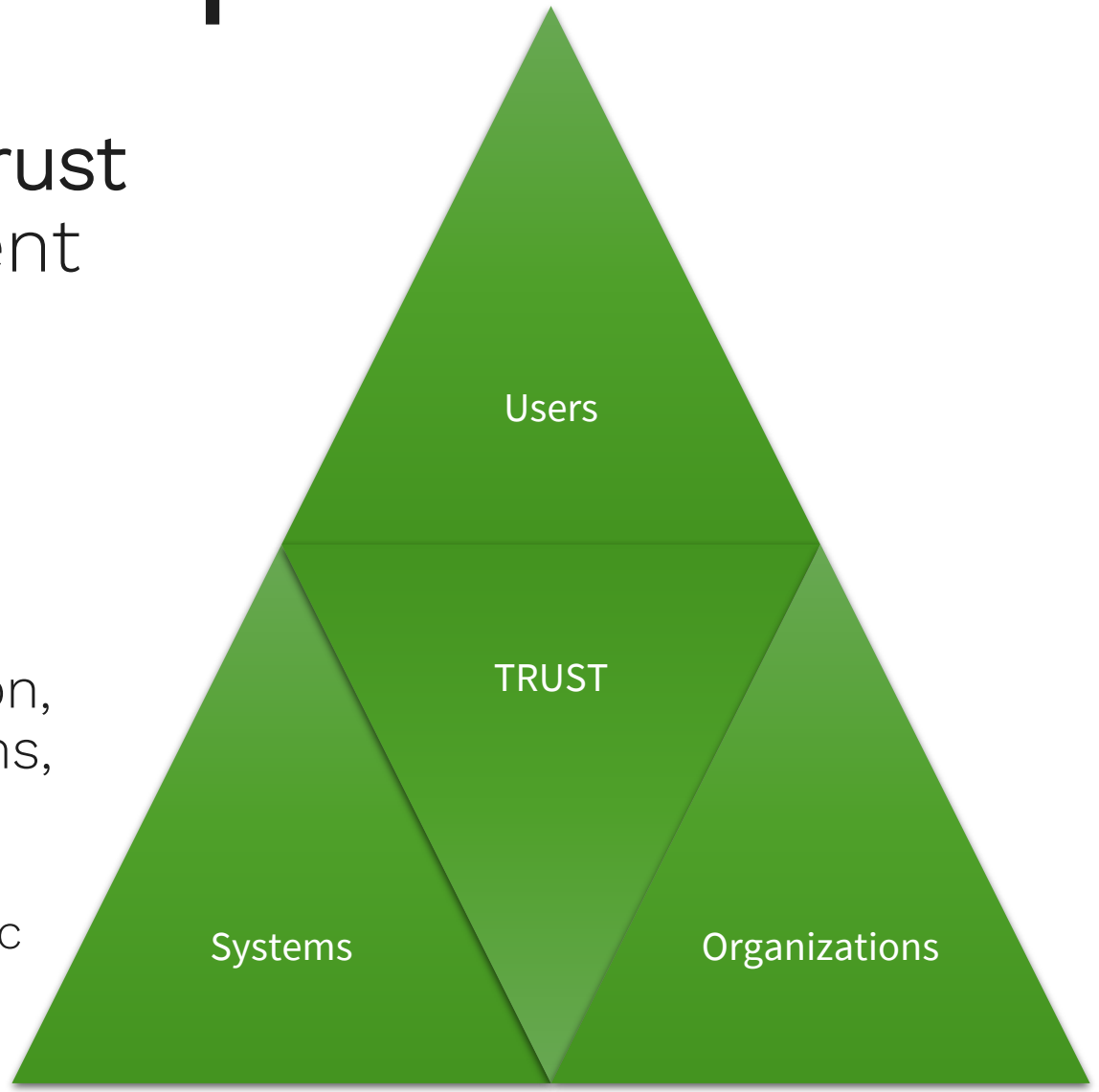
Figures on interoperability and volume of data

- 5.6 million inhabitants in Finland
- More than 3.6 billion documents in Kanta Patient Data Repository
- Customer and patient data of 6.7 million people in Kanta services
- Example: volumes of Kanta prescription service
  - More than 2.5 million prescriptions per month
  - Over 6.9 million dispensations per month

- Connectivity through Kanta services
- Increasingly structured data
- Conformance to national specifications
- High level of trust in security of national infrastructure and service provider systems

Cybersecurity and data protection

- Main principles for maintaining **trust** in health information management
  - Identification and management of risks
  - Respect of privacy
  - Preparation and countermeasures for cyber-threats
  - Requirements for systems and platforms
  - Know-how and support for health and social service professionals
- Spanning through strategy, national legislation, organizational policies, requirements, systems, and technologies
  - General rules and legislation (e.g. GDPR) complemented by social and health care specific rules and requirements



thl

Regulatory framework and governance

National regulations related to essential requirements and certification in Finland (primary use)

Laws (Ministry of Social Affairs and Health)

- Act on the Processing of Client Data in Healthcare and Social Welfare 703/2023
  - Several versions and updates since 2007
- Act on Electronic Prescriptions
  - Latest update 706/2023

Regulatory rules (THL)

- Rule 4/2024: Classification and certification of social and health information systems and wellness applications
- Rule 5/2024: Essential requirements for social and health information systems and wellness applications
- Related: Rule 3/2024 on **information security plans** for health and social service providers

- Previous versions and updates to regulatory rules: 2015, 2016, 2021, 2022, 2023

Some key content in **Act on the Processing of Client Data in Healthcare and Social Welfare 703/2023**

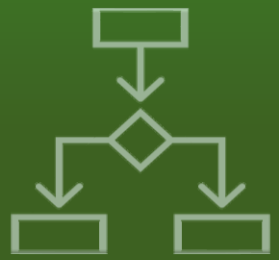
- Definitions, e.g. **health or social care information system**
- **Information security plans** for each health and social service provider
- **Purpose of use** and **classification** of systems
  - A: certified, B: not certified
- **Registration** of systems and wellness applications
- **Conditions for deployment** of systems in production environment
- **Supervision and monitoring** of systems after deployment
- General **responsibilities** of manufacturer and information system service provider
- **Essential requirements** for information systems and wellness applications
- **Compliance and conformance** to essential requirements
- **Interoperability testing**
- **Security audits**
- Supervisory authorities and inspections
- Notifications on **non-compliance** and disruptions
- **Steering, supervision and monitoring**

Essential requirements and certification

Essential requirements in Finnish regulation

Functional requirements

- **Classification** of systems (class A – certification and B – no certification)
- Essential **functions** and essential **content**, references to detailed requirements specifications
- National requirement **profiles** depending on the purpose of the system (EHR, pharmacy, etc.)
- A standard **information form** for **registration** and certification process



Interoperability requirements

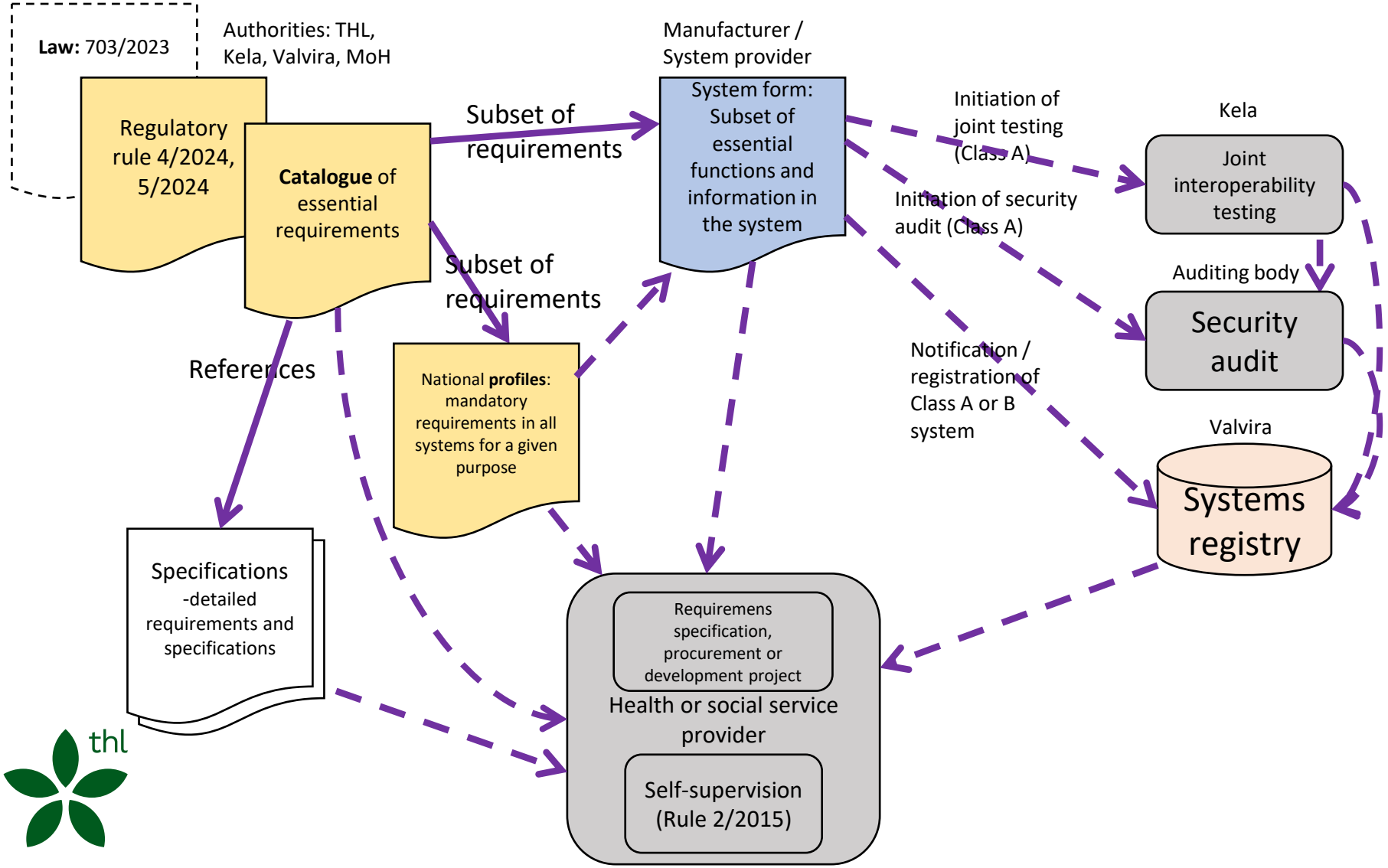
- Requirements and specifications which are relevant for the purpose of the system and national infrastructure (Kanta) requirements
- **Certification - class A2 / A3:** verified through joint testing with Kanta services: connectivity to Kanta services and other connected systems, production and use of data according to specifications

Security and data protection requirements

- **Certification - class A1, A2, A3 :** Verified through external security audit by an accepted auditing body
- Pass: system receives a security certificate (valid for 3 years)

thl

Regulation and use of essential requirements in Finland (since 2014)



- Classification
  - A: certified
    - A1: security only
    - A2: security + interoperability
    - A3: comprehensive (critical or all
  - B: registered (self-certification)
  - Not registered (purpose of use is NOT personal health data)
- Functional profiles
  - 27 national
  - One system may fulfil several profiles

Security subset of essential requirements

Functionalities

- Prescribing functions
- Dispensation functions
- Medical certificate, scanned documents, authorised subcontracting and biobank management functions
- Referral and request functions
- …
- User and access management functions
- Authentication and digital signature functions
- Disclosure and consent management functions
- Access logging functions

Functional requirements for data

- Patient care and electronic health records data
- Social services document management
- …

Security and privacy

- Digital signatures
- Authentication and limitations of professional rights
- Access management
- Access logging and auditing
- User instructions
- Session and care relationship management, management of disclosures and consents
- Application security and resilience
- Resilience, secure transmission and persistence, platform security

In addition, requirement categories for digital services for citizens / patients including health and wellness apps

Certification process in relation to systems development and deployment

Development

- Requirements engineering and system design
- System development
- Documentation*
- Manufacturer's/supplier's self testing

Manufacturer / System supplier

Certification

(Systems connected to the Kanta services and other major systems) (Class A)

- Initiation of certification process*
- Joint testing for interoperability*
- External security audit*, audit certificate

Manufacturer / System supplier

Kela

Auditing body

Deployment, production and updates

- Registration to Valvira, supervisory authority*
- Deployment, deployment tests
- Production and daily use
- Modifications to systems, change notifications*

Valvira

Manufacturer / System supplier

Health care or social welfare organisation

Kela

Auditing body

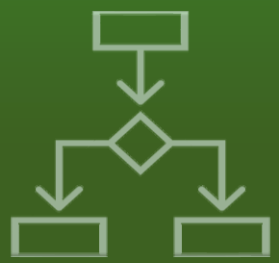
thl

* THL Regulatory rules 4 and 5/2024

Essential requirements in Finnish regulation

Functional requirements

- **Classification** of systems (class A – certification and B – no certification)
- Es
- National requirement **profiles** depending on the purpose of the system (EHR, pharmacy, etc.)
- A standard **information form** for **registration** and certification process



Int

- Requirements and specifications which are relevant for the purpose of the system and national infrastructure (Kanta) requirements
- **Ce**
se

Se

- **Certification - class A1, A2, A3 :** Verified through external security audit by an accepted auditing body
- Pa

Conformance and certification aspects in national regulations since 2014

> 320 registered systems by the supervisory authority

of which ~ 60 certified for security and/or interoperability by a third party, the rest self-certified

each registered system has a subset of >300 essential requirements based on standards and national specifications (in three categories)

27 requirement profiles: collections of minimum requirements of all systems for a specific purpose

including common requirements for EHR systems, eye care systems, dental care systems and imaging systems, social services systems

Authorities related to essential requirements and certification

Operational certification and registration process:

- **Kela -** The Social Insurance Institution of Finland **/ Kanta services**: design, development and maintenance of Kanta services infrastructure
  - **Kanta joint testing**: service: planning and coordination of interoperability testing with systems (class A2 or A3), provides one or more statements from successful testing
- **Security auditors**: accredited companies which perform security audits as part of certification, provides a security audit certificate
- **Valvira** - National Supervisory Authority for Welfare and Health: supervisory authority which **registers** information systems and **supervises** compliance

Steering:

- **Ministry of social affairs and health:** legislation and strategic steering
- **THL** – Finnish Institute for Health and Welfare: steering of information management, including regulatory rules on essential requirements, certification and classification
- **Traficom -** Finnish Transport and Communications Agency: accreditation and monitoring of security auditors

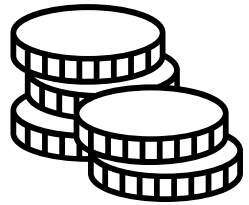
Regular collaboration between authorities for steering and further development of requirements

thl

Reflections and European viewpoints

Experiences of the Finnish certification process

- Mandatory testing and security audit <u>are a burden</u> for system manufacturers
  - Takes time and money
  - Requires careful planning and resources
- The other side of the coin:
  - Product level certification **reduces need for audits and testing from health and service providers** (many large and small health and social service providers)
  - Information security and data protection is perceived crucial by citizens and authorities as well as *most* health service providers and vendors
  - Testing ensures conformance, enabling interoperability and information exchange
  - …across many organisations and systems connected to the national Kanta infrastructure, large volumes of data and searches, large number of different organisations and users



➢ Certification (external testing and security audit) process is an enabler of interoperability and security of all EHR systems, preventing errors and incidents – risk prevention in network of actors and systems

➢ Certification has not been a bottleneck for most systems

➢ About **60 certified (class A)** systems and **more than 320 class B** systems have been registered

Trust risks - case Vastaamo data breach

- Vastaamo: a major private psychotherapy service provider in Finland – 25 therapy centers
- In-house patient information system (registered as class B system → ”self-certification” of essential requirements, not certified by a third party, not connected to the national infrastructure)
- Intruders hacked and stole the patient database in 2018-2019
- Intruders sent extortion demands to the company and to about 30 000 individuals in 2020, threatening to publish patient records, some patient records were leaked in Tor network
- Security practices of the provider and the system were found to be inadequate in investigation
- Some consequences
  - Thousands of victims (many with mental health problems) have suffered anxiety, insecurity and stress from this traumatic event
  - The psychotherapy service provider went bankrupt
  - The ex-CEO of the psychotherapy service provider was found guilty in data protection crime and sentenced to a three-month suspended sentence
  - The suspected hacker was captured in France and has been kept in custody in Finland, facing prosecution on data breach, dissemination of private data and extortion felonies
- New versions of national regulation in 2021 included mandatory security audits to high-risk systems (also other systems than those connected to the national infrastructure)

thl

EU level requirements – cross-border data exchange

- Support for deployment and requirements of national systems related to EU interoperability and security is necessary for **cross-border information sharing** – at this point cross-border ePrescriptions / eDispensation and Patient Summaries are operational in Finland
  - Updates to national specifications for interoperability and data security, updated national profiles (e.g. dispensation requirements for pharmacies)
  - Collaboration and steering of systems connected to national contact point
- MyHealth@EU requirements (eHealth Digital Services Infrastructure) – **cross-border health data exchange**
  - Infrastructure and technical security solutions (e.g. servers and server rooms)
  - Organisational security (e.g. NDAs with system administrators)
  - Documents for security auditing, certified auditors
- National MaCoDeExSe project supports development and updates

thl

European requirements – EHDS and EHR systems

- With EHDS and European Electronic Health Record eXchange Format (EEHRxF) requirements are increasingly extending towards local and national systems
- EHDS requirements on European level - for **EHR systems**
  - Functional requirements related to identification, authentication and authorisation for EHR systems
  - Access rights and retention period management for categories of health data
  - Harmonised logging component for EHR systems
  - Implementing acts and further specifications for cybersecurity, confidentiality and integrity of electronic health data
  - Secure processing environments for secondary use of health data
- Level of security and privacy requirements and certification in EHDS (alone) is not on comparable level in relation to Finnish national requirements
- Requirements in EHDS, Cybersecurity act, Cyber-resilience act, GDPR, MDR, NIS2

thl

Reflections and recommendations

- Regulations related to data security and protection are scattered across several European and national regulations
- It is important **not to introduce overlapping but harmonised** requirements and procedures through EHDS, MDR, NIS2, Cyber-Resilience Act, Cyber-Security Act and GDPR…
- In competitive markets, third-party involvement and market surveillance are often necessary to **ensure compliance** and **fixing of identified deficiencies and risks**
  - Jointly agreed specifications and after-the-fact supervision alone can not guarantee that all parties act in accordance with the requirements
  - While EHDS conformance and compliance relies on self-assessments, EHDS does not prevent complementary requirements and certification on national or European level

thl

Summary

Summary

- Finland has long tradition and experience on national level information exchange and certification of systems
- Both interoperability and security must be ensured
  - Conformance and verification must be detailed enough
- In Finland, **trust** in interoperability, security and confidentiality of systems and health data exchange has been seen as an imperative
  - In addition to and on top of international standards and specifications, complementary national requirements or activities have been necessary
    - specifics in organization of health services, critical national infrastructures and data repositories
  - EHDS enables also national safeguards and certification practices for aspects other than harmonised EHR components
- Despite European and national requirements, security and confidentiality risks must always be mitigated on local level

Thank you!

sote-tiedonhallinta@thl.fi

MaCoDeExSe project is funded by European Union under EU4Health Programme

Funded by the European Union