Norwegian TREs towards EHDS:

Defining and testing SPE requirements

NORTRE

EOSC-ENTRUST blueprint roadmap workshop
8th May 2024

Christine Stansberg
Group leader Sensitive Data
IT division
University of Bergen

Content

- Background
- Defining SPE requirements
- Testing requirements on Norwegian TREs
- Outcomes
- Next steps

EHDS – European Health Data Space

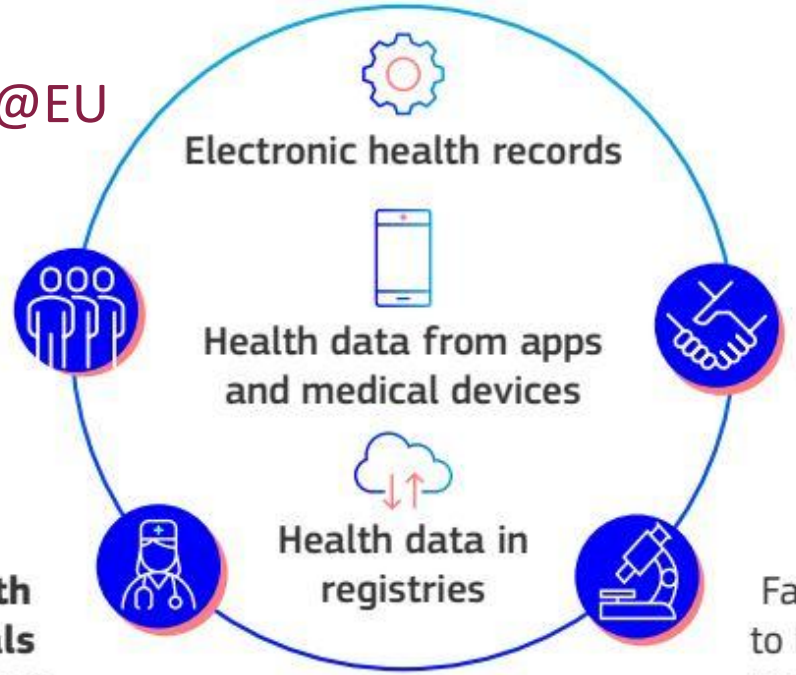
Primary use: MyHealth@EU

Better diagnosis and treatment:

- improved patient safety
- continuity of care
- improved healthcare efficiency

Empower **individuals** to have control over their health data

Enable **health professionals** to have access to relevant health data

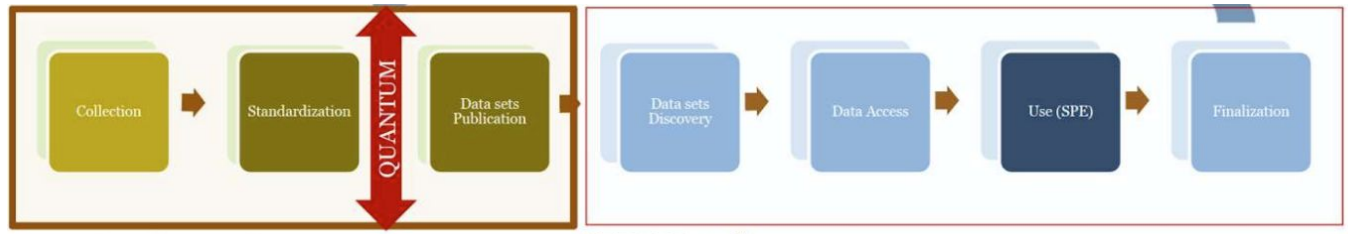


Assist **policy makers and regulators** in accessing relevant health data

Facilitate access to health data for **researchers and innovators**

Better health policy, greater opportunities for research and innovation

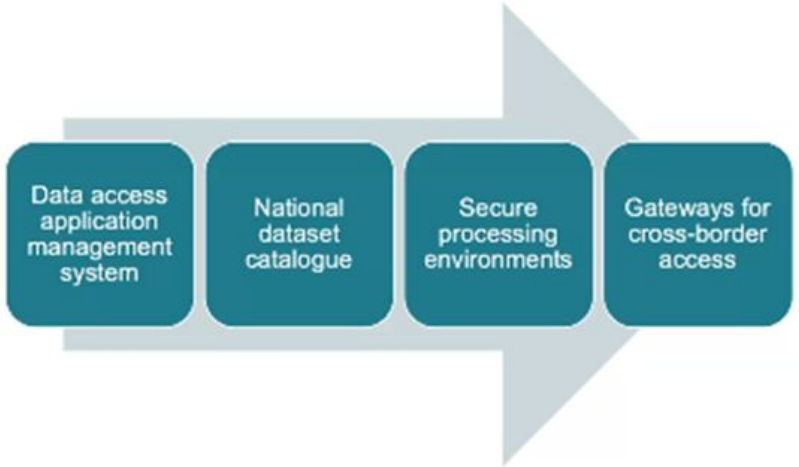
Secondary use: HealthData@EU



Data holder role **HDAB role**

HealthData@EU - Secondary use of health data

Four Digital Business Capabilities to be deployed:



Articles of the European Health Data Secure processing env

Article 50, Secure processing environment, Articles of the European Health Data Spa

1. The health data access bodies shall provide access to electronic health data only throu organisational measures and security and interoperability requirements. In particular, th

(a) restrict access to the secure processing environment to authorised persons listed in t

(b) minimise the risk of the unauthorised reading, copying, modification or removal of el environment through state-of-the-art technological means;

(c) limit the input of electronic health data and the inspection, modification or deletion c environment to a limited number of authorised identifiable individuals;

(d) ensure that data users have access only to the electronic health data covered by their identities and confidential access modes only;

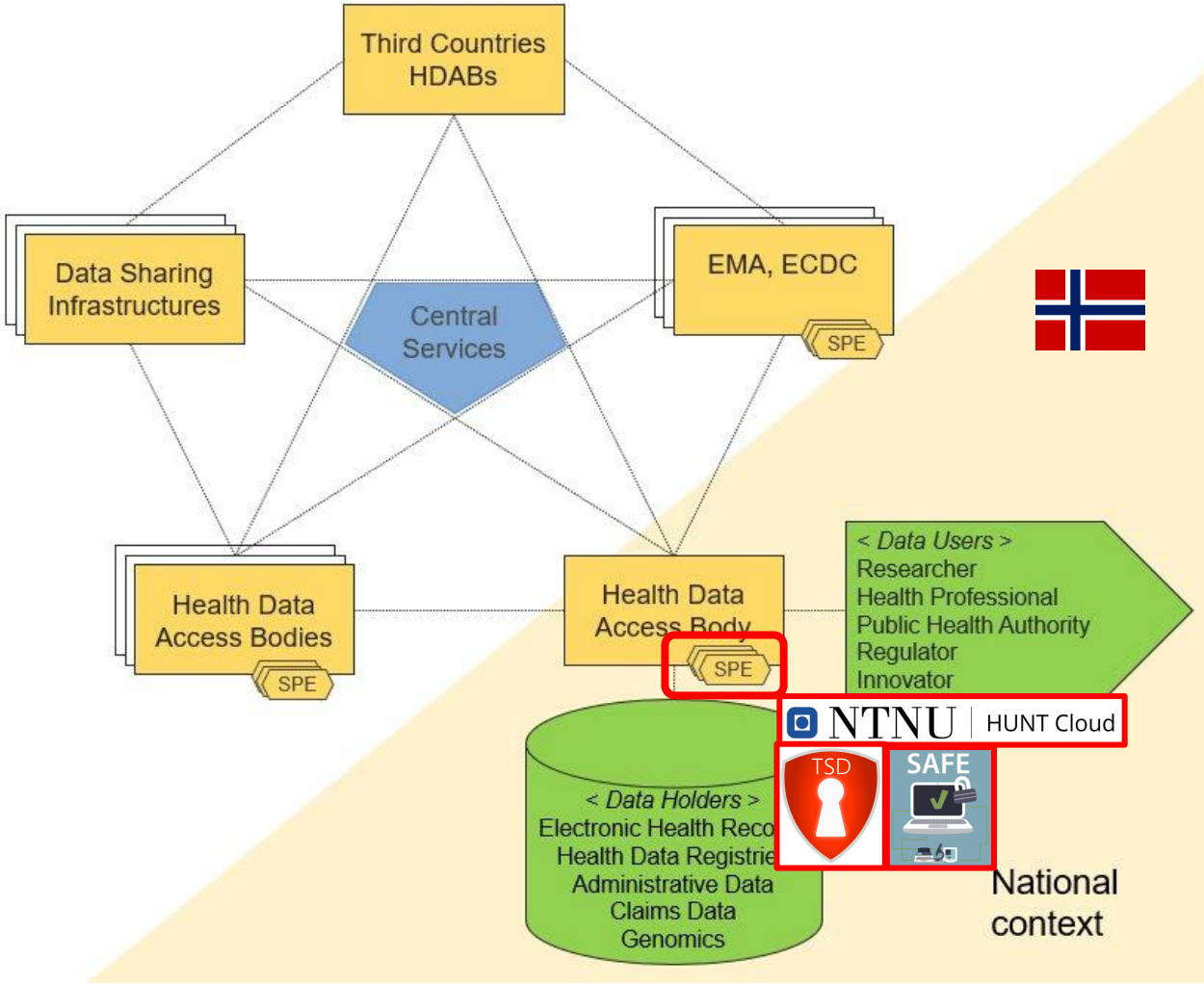
(e) keep identifiable logs of access to the secure processing environment for the period c operations in that environment;

(f) ensure compliance and monitor the security measures referred to in this Article to mit

2. The health data access bodies shall ensure that electronic health data can be uploaded a secure processing environment. The data users shall only be able to download non-pers environment.

3. The health data access bodies shall ensure regular audits of the secure processing envir

4. The Commission shall, by means of implementing acts, provide for the technical, information security and interoperability requirements for the secure processing environments. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2).



Source: European Health Data Space (europa.eu)

NORTRE

Norwegian Trusted Research Environments

- Collaboration between UiO, UiB and NTNU
- Commissioned by national health authorities to provide SPEs for analysis of health data
  - «Thrifted solution» after failure of national health analysis platform platform
- Sparked idea to collaborate closer on providing
  - Secure storage and analysis with federated trust between platforms
  - Simplified data movement between platforms
  - Interoperability between platforms
  - “EHDS ready” SPEs

NTNU | HUNT Cloud

SPUHiN

FAIR Secure Procurement and Use of Health data in Norway (2023-27)

Aims:

To further develop the following capabilities within Norway:

- National dataset catalogue
- Gateway for cross-border access
- Secure processing environments (SPE)
  - Develop requirements and verification procedures
  - Support the existing TREs in the project to comply with requirements
    - Report first year: Lundgren et al. 2024

Overall goals for requirements

Standards based	Standards like ISO/IEC 27001 already recognised and in broad use. Building on certification according to existing standards, can ease the process for both SPEs and auditors.
Meets the risk	Requirements need to be in line with the cyber security and privacy risk related to SPEs.
In line with European requirements and initiatives	SPEs need to meet requirements described in EHDS, specifically Article 50. Also beneficial to be aligned with other European countries.
Flexible, able to handle changes in technology and risk	Technology- and risk landscape constantly changing, needs to be considered when selecting the requirements.

Modified from Lundgren *et al*. 2024

Preparing for requirement selection

1. Review of existing relevant standards
2. Threat modelling of a general TRE infrastructure
3. Review of EHDS requirements and relevant outcome of related activities

1. Review of standards

Standard / framework / etc.	Summary assessment
ISO/IEC 27001 and 27002	Internationally recognised standard for general information security. Certification process available and relatively widely used among IT service providers. Scope and risk level is however determined by each entity. Harmonisation in this area may be needed to ensure sufficient level of trust from use of this standard and certification scheme.
ENISA Cloud services cyber security certification scheme	The cloud security cyber security certification scheme concerns information security in an IT provider setting, but not all SPE providers can be considered as cloud services and the framework is relatively heavy. The development of cyber security certification schemes governed by ENISA would however be very interesting to consider if certification of SPE's will be required. Perhaps development of a scheme for SPE / Trusted Research Environments (TRE) could be discussed.
Guideline on «State of the art» from Germany	Focusing on what technologies that are considered «state of the art» with focus on compliance with the German IT Security Act and GDPR. It is not intended as a check list or complete list of security measures to implement. It may however be a good tool in discussions on what type of technical implementation of security measures that is sufficient in the SPE setting. Especially since the state-of-the-art concept is used in 1b in the Article 50 of EHDS.
Building Trusted Research Environments – Principles and Best Practices («Five safes» report) from the UK	The general concepts for TRE and the five safes are also very relevant for EHDS, including the SPE concept. It may provide a good basis for discussion on requirements that are specifically important to safeguard for SPE's. It is worth noting that it refers to ISO27001 when it comes to governance framework.
Data protection Code of Conduct for Cloud Service Providers	The Code of Conduct describe required concepts on a relatively general level and may be difficult to use directly to define requirements. As mentioned earlier not all SPE's will be able to categorise as cloud service providers.
Finnish regulation 1/2022, including «Annex 1: Requirements for a Secure Operating Environment» and Katakri	There is a robust set up of regulation with detailed requirements both for the SPE providers, the accreditation and certification process. It does not however seem to be easily mapped to established standards. It would be very interesting to learn from the Finish experiences with both advantages and disadvantages with their set up.
French regulation	Limited review performed since the regulation is not available in English. Similar to the Finnish regulation it would be interesting to learn from the French experiences with their set up.
NIST Cyber Security Framework (CSF), NIST SP 800-53	The NIST framework is widely recognised and used internationally although it is American. The initial assessment is however that an international standard such as ISO may be more feasible to implement in a European setting.
The Norwegian «NSM grunnprinsipper» and «Normen»	We have mainly focused our assessment on standards that are used across Europe. These are however good examples of local implementation of good practice.

2. Threat modeling

- Description of the system – what is it that we want to protect?
- Identification of potential threats to the system – what can go wrong?
- Identify mitigations – what can be done?

- Developed together with the analysis infrastructures HUNT Cloud, SAFE and TSD
- Individual meetings with TSD, SAFE and HUNT Cloud. Modeling of DFD by the Directorate of e-health in-between meetings
- Goal: high level general overview

- Topic for discussion: What can go wrong?
- DFDs used as a basis for the discussions
- Participants from the Directorate of e-health and HUNT Cloud, SAFE and TSD

- Goal: to identify the main findings from TM workshop 1, and identify areas where more discussion was needed
- Performed by the Directorate of e-health

- Presented and discussed findings and open issues
- Participants from the Directorate of e-health and HUNT Cloud, SAFE and TSD

- Documented the results from the threat modeling
- Performed by the Directorate of e-health

Modified from Lundgren *et al*. 2024

3. Related EU requirements and activities

input specifically relevant to EHDS

- EHDS regulation, specifically requirements in article 50
- TEHDAS WP7 – Connecting the dots, specifically
  - Milestone 7.6 and Deliverable 7.2 – with guidelines for SPEs and interoperability requirements
  - Questionnaire to existing SPEs should build on existing standard + EHDS
- EHDS2 Pilot WP7 – Regulatory and legal compliance, specifically
  - Deliverable 7.2 – Relevant information on SPEs included in section on Data use
  - Questionnaire summary related to data provision and use
- Workshop ”Elements of Secure Processing Environments” by EOSC-Life and HealthyCloud (June 2023)
- BBMRI-ERIC Security and Privacy Architecture

Modified from Lundgren *et al*. 2024

Requirements (1/3) 15 in total

Primarily security related requirements

No	Requirement description	Priority
R1	The SPE provider operates an information security management system (ISMS) according to ISO/IEC 27001. The scope of the ISMS covers the SPE provider's organisational units, locations and processes for providing the SPE infrastructure.	High
R2	The SPE provider has policies and systems for digital access control (including identification, authentication and authorisation) on a security level that is in line with the level of risk. Risk related to privileged access control is managed.	High
R3	Possible processes for import of health data (both digital and manual processes) are identified and sufficiently secured in line with the level of risk. The communication channels within any distributed SPE infrastructures are set up in a secure manner.	Medium
R4	Services for extracting data from the SPE only allow for extract of non-personal health data.	High
R5	Where cryptography is used, the key length, strength of encryption algorithms and key management is in line with the risk level, also considering how long the cryptographic protection needs to last.	Medium

Lundgren *et al*. 2024

Requirements (2/3)

Primarily security related requirements

No	Requirement description	Priority
R6	The SPE provider performs logging and monitoring on a level that makes the SPE provider capable to discover the most important types of unwanted events that has been identified in risk assessments.	Medium
R7	The SPE provider continuously backup digital assets and the backups are protected against unauthorised access.	Medium
R8	Health data is sufficiently secure during storage and storage equipment is protected during its whole lifetime (including decommissioning).	Medium
R9	The SPE provider is prepared to manage information security incidents.	Medium
R10	The SPE provider has a documented security architecture that meets the identified needs of SPEs, including of segregation between SPEs within the SPE infrastructure. Both physical and digital security is a part of this architecture.	High
R11	The SPE provider has a documented and established good practice for secure operations of the SPE infrastructure.	Medium

Lundgren *et al*. 2024

Requirements (3/3)

Purely functional requirements

No	Requirement description
R12	The SPE provider has documented standard analysis capabilities or tools that are available to the user. The SPE provider has processes for secure import of new or updated tools based on user needs. The SPE provider has processes for license management.
R13	The SPE provider has documented and established good practice for support, maintenance and development for the SPE services.
R14	The SPE provider has documented and established services for archiving or secure integration with archiving systems.
R15	The SPE provider has documented and established secure services for persons and/or systems to interact with the data and tools for analysis.

Lundgren *et al*. 2024

Test plan

- ISO27001 certified vs non-certified TREs
  - evaluate the benefit of leveraging on an existing certification.
- High-priority requirements were more extensively tested
- External consultant “auditor”

- Relatively high-level requirements, gave few details on HOW to implement
- NB - Not testing compliance related to the responsibility of the *data users*.

Modified from Lundgren *et al*. 2024

Summary of results

- No formal minimum requirements for SPEs
  - focus on how well TREs have implemented the tested requirements
- Five areas especially relevant to SPEs and data users:
  - Information security management system
  - Access management
  - Data export
  - Data import
  - Functional requirements
- All TREs have high focus on both functionality and security.
- Operate with different setups
- Some gaps – exemplified by SAFE in next slide

TRE example: SAFE

Area	Summary Results
Information security management system	a) Not ISO 27001 certified but is a part of the ISMS by UiB. b) Missing the connection between UiB ISMS and SAFE's security work. c) Several routines missing formalization and/or documentation.
Access Management	a) Access is set up by SAFE, based on an access document in excel administered by the project owner. b) The project owner has the possibility to review access by running a script, and manually through the access document. c) Access logs are available upon request. d) Norwegian users require a UiB account, authenticated using MinID. Foreign users are allowed access after project owner approval. The project owner is responsible to perform authentication using at least one type of identification number. e) It is possible to granulate access on file-level in a project. f) All users must have an UiB account, where they sign the ICT-rules, security information and privacy statement for UiB.
Data Export	a) Secure export function available by using a personalised export-folder. b) Project owner controls who has access to export. File is encrypted and must be opened with a password only available to the user. c) Project owner has access to export logs. d) A copy of the exported file is retained. The project owner can request that export needs to be approved before it is exported.
Data Import	a) Secure import function by using a personalised import-folder. b) Machine to machine transfer is available. Not generally set up between register to analysis infrastructure.
Functional requirements	a) Provide a basis set of analysis tools and have procedure for adding more tools if requested. b) Internet connection not allowed. Provide mirrored versions of tools that requires internet connection. c) UiB provides some license for all UiB-accounts and SAFE distributes licenses to all fixed analysis tools, Outside of this license management is based on "Bring-your-own-license"

Modified from Lundgren *et al*. 2024

Next steps

For Norway:

- Agree on minimum requirements for SPEs
- Formalise national guidelines for SPE users and providers based on these
- Implement national process and mechanisms for verification of compliance
- Represent all relevant stakeholders in further process, including potential providers

For NORTRE in particular, closing gaps:

- Improve ISMS, to prepare for potential ISO 27001 certification
- Adjust to emerging minimum requirements for SPEs
- Implement eDelivery for machine-to-machine transport between data holder and SPE.

Thank you!

People involved:

Organisation (in 2023)	Core team
Directorate of e-Health	Klara Lundgren Anne Heidi Skogholt Inger Anne Tøndel Tonje Stegavik Olav Astad Kristiansen
Norwegian Institute of Public Health	Elisabeth Hagen
Directorate of Health	Tricia Larose
EY (consultant)	Birgitte Fjærestad

Organisation	Contributors
TSD @ UiO	Gard Thomassen Leon Charl du Toit Haneef Awan Frode Strømsvåg
HUNT Cloud @ NTNU	Oddgeir Lingaas Holmen Tom-Erik Røberg Qussay Ghazeia
SAFE @ UiB	Christine Stansberg Haakon Fannemel Breivik Tore Linde Askil Laastad Jarl Magnar Hansen Kristoffer Baldysz Erling Langøigjelten

Pathway to requirements

Evaluated ISO controls

01

Evaluated all ISO/IEC 27002 controls (Low/Medium/High)

- Is this control of particular relevance to SPEs (as compared to other types of IT-systems)?
- Is this control directly important to fulfil requirements in EHDS article 50?
- Is this control of particular relevance to the risk highlighted in the threat modeling workshops?

Identified relevant controls

02

Identified the most relevant ISO/IEC 27002 controls (and groups of controls)

Compared controls

03

Compared the identified controls to what is proposed by other initiatives

- Are the same controls covered there?
- Something missing in our controls?

Mapped to EHDS requirements

04

Revised suggestion – mapped the identified controls to EHDS article 50 requirements

Added functional requirements

05

Added functional requirements

Discussed with stakeholders

06

Discussed the suggested controls with stakeholders, and revised as needed

Lundgren *et al*. 2024

Example test plan (1/4)

High priority requirement, certified entity

R1	The SPE provider operates an information security management system (ISMS) according to ISO/IEC 27001. The scope of the ISMS covers the SPE provider's organisational units, locations and processes for providing the SPE infrastructure.	Verify per inspection that the SPE provider has a valid certificate for ISO/IEC 27001.	* ISO/IEC 27001 certificate
		Verify per inspection of the scoping documentation that the relevant organisational units, locations and processes for providing the SPE infrastructure are included.	* Scope of the ISMS
		Verify per inquiry and inspection of the results from the last management review that there is focus on continuous improvement and management accountability and involvement.	* Results of the last management review

Example test plan (3/4)

High priority requirement, non-certified entity

R1	The SPE provider operates an information security management system (ISMS) according to ISO/IEC 27001. The scope of the ISMS covers the SPE provider's organisational units, locations and processes for providing the SPE infrastructure.	Verify per inquiry and inspection of relevant documentation that essential elements of leadership commitment in the ISMS are in place, e.g.: * Leadership and commitment * Policy * Organizational roles, responsibilities and authorities	* Information security policy established by top management * Example of top management communication the importance of information security and conforming to the ISMS requirements * Documentation on how information security responsibilites and authorities are assigned
		Verify per inquiry and inspection of relevant documentation that planning of the ISMS is based on risk and that information security objectives have been established.	* Documentation of security objectives * Documentation of information security risk assessment process * Example of significant information security risk assessment
		Verify per inquiry and inspection of relevant documentation that there is sufficient resources and competence to support the ISMS, and that there are procedures for continuous awareness training.	* Documentation of assessment of resource and competance needs * Awareness training plan
		Verify per inquiry and inspection of relevant documentation that there are procedures for evaluating the performance of the ISMS, e.g. trough: * Monitoring procedures * Internal audit * Management review	* Documentation of information security monitoring results * Latest internal audit report * Latest management review report
		Verify per inquiry and inspection of relevant documentation that there are procedures for continual improvement.	* Documentation of the procedures for continual improvement * Example of nonconformity report and corrective actions