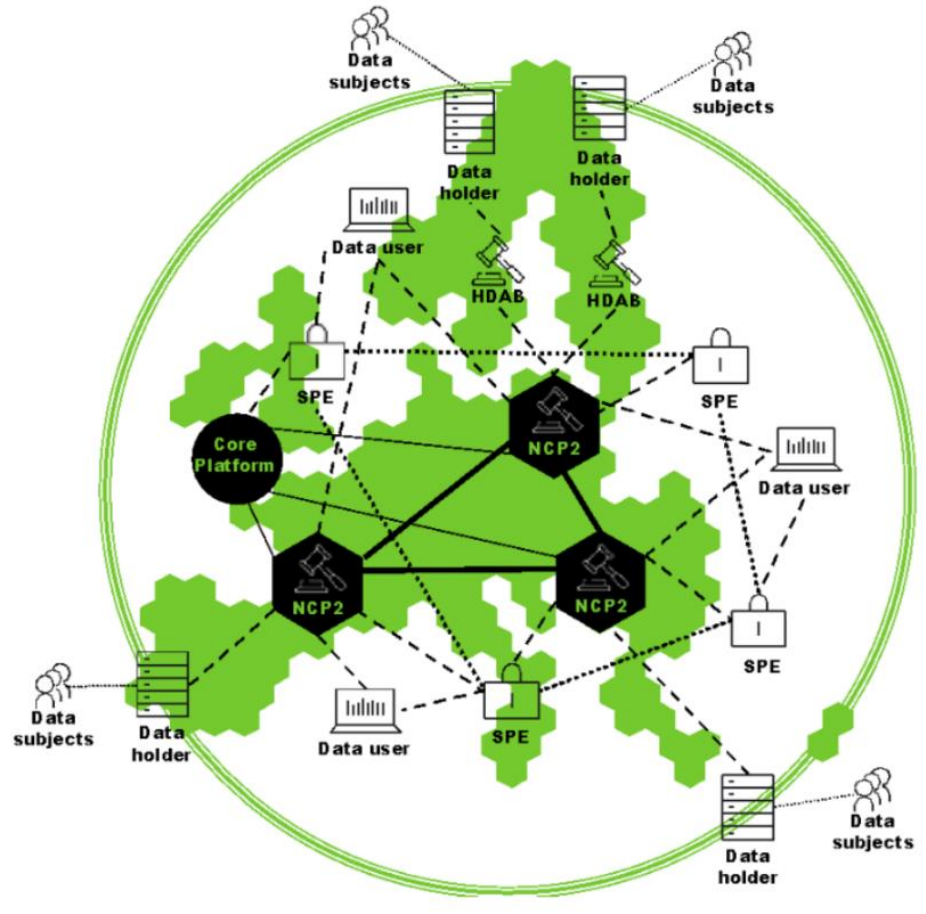
Helsedirektoratet NIPH

Co-funded by the European Union

GAP Analyses

GAP Analyses for secure data transport in secondary use of Health Data

Delivery | EU4H-2022-DGA-MS-IBA-4 — Direct grants to Member States: for setting up services by Health Data Access Bodies - Secondary use of health data



Helsedirektoratet NIPH Co-funded by the European Union

Document information

Authors (Work Package 8):

Name	Organisation
Line Andreassen Sæle	Norwegian Institute of Public Health
Hans Aage Huru	Norwegian Institute of Public Health
Geir Kristian Hansen	Norwegian Directorate of Health
Arne Dybdahl	Norwegian Directorate of Health
Olav Astad Kristiansen	Norwegian Directorate of Health

Accepted in the Advisory Board November xx

Version 1.0

Project number: 101128232
Milestone: D8.2
Date: 28.11.2024

Helsedirektoratet NIPH Co-funded by the European Union

Contents

Introduction

This document provides a description of the current, the desired architecture and addresses the gap to secure health data for secondary use from registries to the secure researching environment in Norway. The aim is to establish a target architecture and a roadmap for the development of services necessary for the transport of health data for secondary purposes. Data for secondary use, here are to be interpreted as categories mention in Article 51 in EHDS Regulation.

This target architecture aims to be applicable for the EU initiative HealthData@EU and to represent the baseline for further work in the FAIR Secure Provision and Use of Health Data in Norway (SPUHiN) project. All deliverables in the SPUHiN project will be measured based on baseline. And as part of the name, the FAIR principles of findability, accessibility, interoperability, and reusability (FAIR) are vital to comply with.

HealthData@EU is an initiative by the European Union to create a digital infrastructure for the secondary use of health data across Europe. This initiative is a part of the broader European Health Data Space (EHDS) initiative and regulation and aims to facilitate the FAIR sharing and use of health data for research, innovation, policy-making, and regulatory purposes in Europe.

HealthData@EU re-uses eDelivery infrastructure[1] and will connect various data platforms from EU member states, enabling a secure and standardized way to access and utilize health data for secondary use.

[1] press release from EU Data sharing through eDelivery in the HealthData@EU

This GAP analysis is mainly based on the secure transport of health data for secondary use and focuses mostly on how health data is transported from a Data Holders to a Secure Processing Environment infrastructure. The EHDS regulation will impose such requirements on both Data Holders and analysis infrastructures in the future. It is important for us to work together with data holders and analysis infrastructure providers to address the national challenges, so that by the time the regulation comes into effect, the Norwegian infrastructure will be ready in place.

Identified GAPs are at the capability level from current level and between the desired level and they are categorized into four main areas. Identified GAPs are at the capability level categorized into four main areas as roles.
The first role is HealthData@NO Administrator, the second is SPE provider, the third is Data Holder and the last is the role of researcher. The identified GAPs are listed within the above categories.

Helsedirektoratet

NIPH

Co-funded by the European Union

Chapter 1

Summary

1. Summary

Making the most out of the data, information, and knowledge of Health available for analytics, research and continuously improvement, this needs to be distributed swift, smart, and safe. This document presents a target architecture and way to get there.

In short, desired state for a target architecture holds keywords and areas as New Secure Infrastructure, Secure Communication Channels, Encryption and Anonymization, Logging and Monitoring, Regulatory Requirements and Compliance, User-Friendly for Data Holders, and secure processing environment (SPE) suppliers. Key principles and solutions for this target architecture; Automation of Data Collection and Preparation, Support for Collaboration and Cooperation, Integration of Security and Privacy Protection in the architecture and Standardization of Data Quality and Formats.
As of end of 2024, the situation for Secondary Use of health data in Norway slow access due to burdened bureaucratic case processing, manual work for extraction and distributing the data, and a somehow currently fragmented network, system, and storage landscape.
This analysis addresses the capabilities and GAP of the four roles; 1) HealthData@NO Administrator, with capabilities as Standardisation of capabilities, Manage shared services and The ability to do health data privacy assessment. Additionally, it is essential to facilitate the exchange between HealthData@NO and HealthData@EU. - 2) Secure Processing Environment-provider, capabilities as Receiving Health Data, Distribute Health Data and Analyse Health Data - 3) Data Holder, capabilities as Prepare Health data for delivery, Delivery health data and Health data information management and - 4) Researcher organisation capabilities for Agreements with SPE Provider organisation, managing ID-address to the SPE and conduct and manage Data Protection Impact Assessments and Data management plans.

Chapter 2

Desired State

2. Desired State

This chapter, desired state describes what abilities secure transport of health data for secondary usage demands and will use as a target architecture.
The prerequisite for the planned Norwegian infrastructure is that eDelivery can satisfy the desired need for Data Holders and Secure Process Environments

In Norway, the secure transport of data is crucial for safeguarding privacy and ensuring the integrity of health data for secondary use, for use in statistics, health analyses, research, quality improvement, planning, management, and preparedness to promote health, prevent disease and injury, and provide better health and care services. Norway is planning to implement mechanisms and procedures to ensure that health data transfers occur in a more safe and regulated manner.

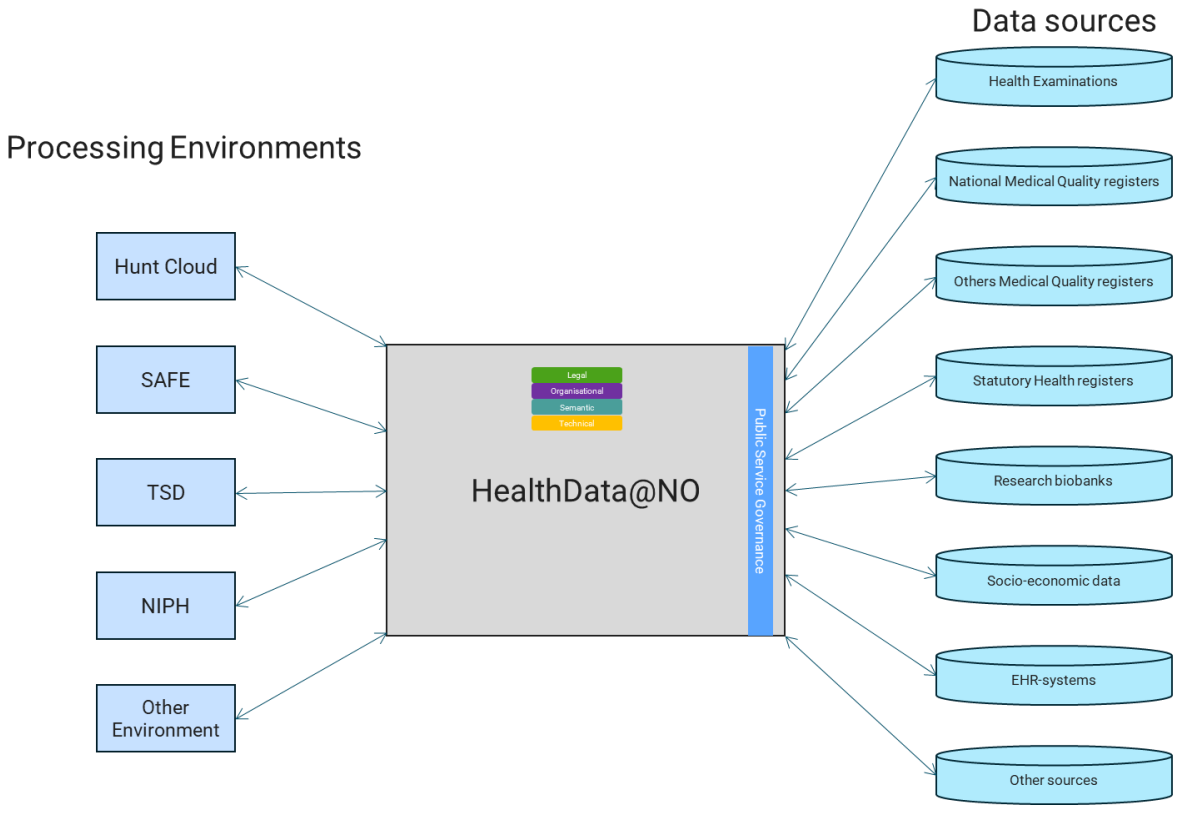


Figure 1 The planned Norwegian infrastructure.

Data security should be encrypted end-to-end, and it should be easy to connect both new Data Holders and analysis infrastructures. The actors or roles in the network will log all traffic and are obliged to exchange data with each other.

The project needs to establish a guide in the use of standards in eDelivery"

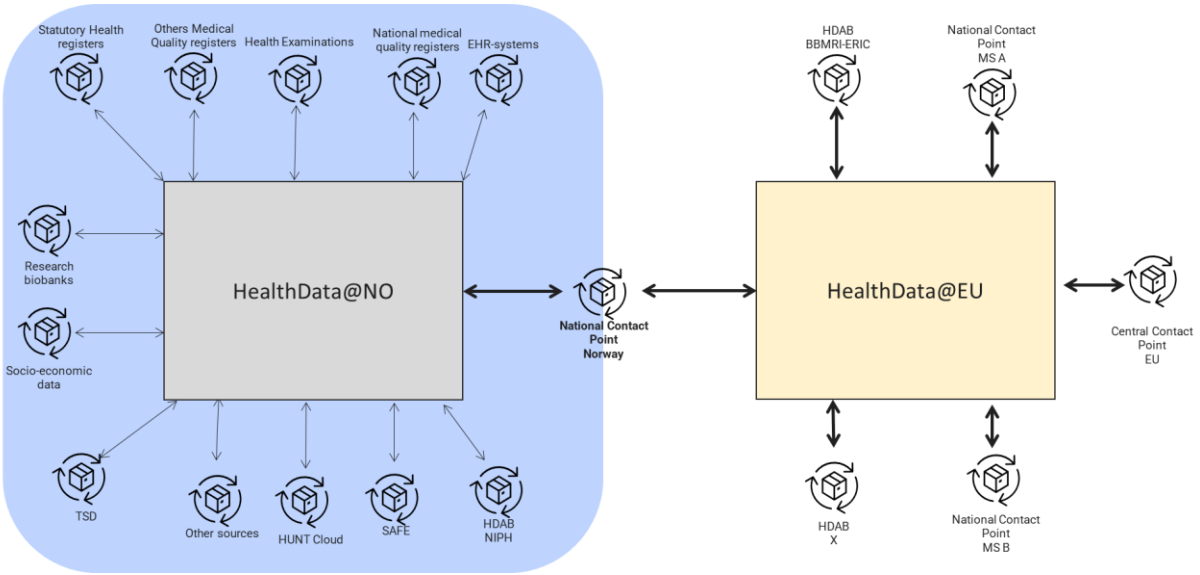


Figure 2 The planned Norwegian infrastructure in collaboration with HealthData@EU.

The EHDS initiative/regulation requires one national contact point per country to connect to HealthData@EU, and a national network should be able to connect to HealthData@EU through the national coordinating Health Data Access Body (HDAB). The national coordinating HDAB has a significant role in being the bridge between HealthData@NO and HealthData@EU.

Here follows a synopsis of the target architecture:

New Secure Infrastructure

Secure transport of health data for secondary use in Norway will be crucial for safeguarding privacy and ensuring the integrity of data used for research, health monitoring, quality improvement, and other secondary purposes. Norway is planning to implement common procedures and mechanisms to strengthen common services, processes, and procedures to ensure that data transfers occur in a safe and regulated manner. This will always follow the intentions of the EHDS regulation.

Secure Communication Channels

Health data for secondary use should be encrypted from data holder and transferred via secured communication channels. The eDelivery technical infrastructure[2] ensures safe and efficient data transfer between health and socioeconomic data registers, research institutions, and authorities, minimizing the risk of unauthorized access or data theft during transmission.

Encryption and Anonymization

Before health data is transmitted, from a Data Holder to a SPE it will be anonymized or pseudonymized so individual identities cannot be directly traced. The data will be encrypted both during transmission and storage, ensuring that even if the information were intercepted, it would remain indecipherable without the correct decryption key.

Logging and Monitoring

Contact Points will log and monitor all data transfers to detect and respond to any irregularities or security breaches. This allows data activity to be tracked and audited, enhancing accountability and compliance with legal requirements.

Regulatory Requirements and Compliance

The transport of health data for secondary use should comply with strict regulatory requirements, including the EHDS regulation, The Health Register Act (Helseregisterloven), The Personal Information Act (Personopplysningsloven), The Security Act (Sikkerhetsloven), The Norwegian Code of Practice for Information Security in the Health and Care Sector (Normen) and General Data Protection Regulation (GDPR), to mention a few.

User-Friendly for Data Holders and SPE suppliers

For health data to be used for secondary purposes and in SPE with user-friendly solutions, several factors and technological measures need to be implemented. These measures can simplify access, analysis, and sharing of health data while ensuring compliance with privacy and data security, this is a part of WP5 in the SPUHiN project.

Integration of Security and Privacy Protection in the architecture

Privacy and data security must be integrated into the architecture. This could include encryption and access controls that are easy to use but still meet the requirements of European Health Data Space (EHDS), GDPR, and national regulations. Secure

[2] Press release from EU Data sharing through eDelivery in the HealthData@EU

processing environments should also have access to training and guidance on best practices for data processing and privacy protection.

This work aligns with the principles and recommendations outlined in the European Interoperability Framework (EIF), which provides specific guidance on setting up interoperable digital public services

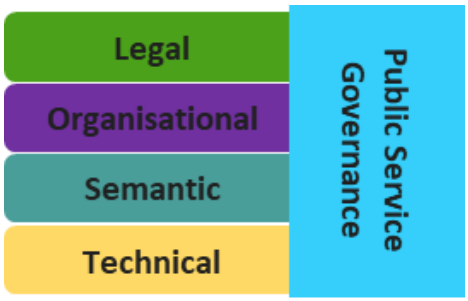


Figure 3 European interoperability framework (EIF)

Helsedirektoratet

NIPH

Co-funded by the European Union

Chapter 3

Current Situation

3. Current Situation

As of end of 2024, the situation for Secondary Use of health data in Norway slow access due to burdened bureaucratic case processing, manual work for extraction and distributing the data, and a somehow currently fragmented network, system, and storage landscape.

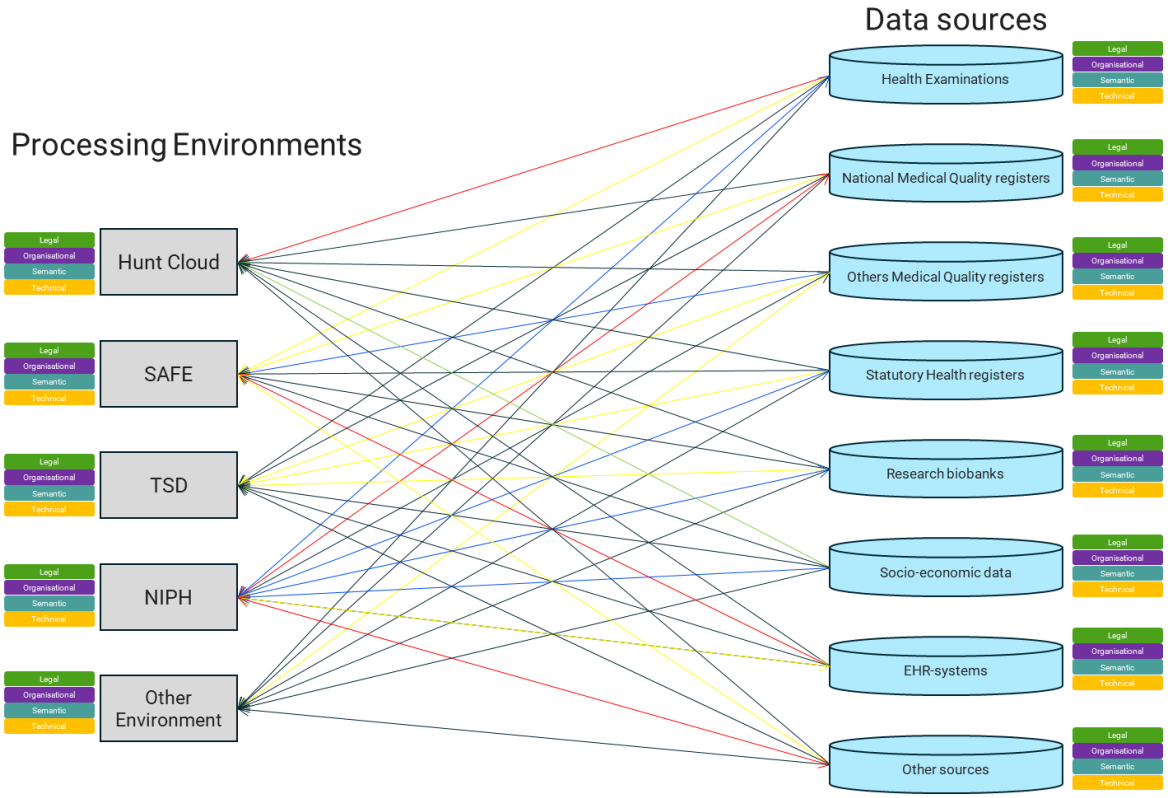


Figure 4 The current situation regarding data transfers

Secondary Use of health data in Norway refers to how health information is collected, processed, and utilized for purposes beyond primary use. Secondary use may include research, statistics, quality assurance, health planning, and policy making. Secondary use of health data is carefully regulated to ensure that data is used in a manner safeguarding patient privacy and data security.

Data Collection and Storage

Health data in Norway is collected from various sources, including hospitals, general practitioners, and other health services. The data is stored in national health registers. The Health Register Act (Helseregisterloven) and the Personal Information Act (Personopplysningsloven), regulate how data is collected, stored, and used, and the Norwegian Data Protection Authority (Datatilsynet) is responsible for supervision.

Data enrichment and quality assurance

Adding or aligning basic information about the persons found in the register (e.g., name, birthdate, etc.) with authoritative sources, such as The National Population Register.

Ensuring further correctness and completeness of the dataset this can include:

- checks across registers (e.g., the Cancer Registry and the Cause of Death registry have processes which help ensure that all persons who have died with any cancer diagnosis are or become included in the Cancer Registry).
- requests back to data sources for data which is missing or inadequate
- checks against expected trends or deviations within the dataset

Data preparation

Transforming and packing the data into different kinds of data products, to simplify re-use within downstream, data management and data utilization processes. Such processes may include:

- standardization according to various consumer requirements, data coupling or aggregation
- anonymization or pseudonymization (see below), etc.

Anonymization and Access Control

Before health data can be used for secondary purposes, they have to be pseudonymised, anonymised and minimised. If there still are risk of identifying patients' health data, they will be aggregated or not delivered to users.

Organizations and researchers must apply for access to the data. Only when an application for health data for secondary use has been approved by an ethics committee and the application for the same data has been approved by the data holders will they be able to be disclosed.

Only the applicant who has been granted permission to use health data will be able to access the data, which will be controlled by the various SPE infrastructures.

Applications

Health data is used for several important secondary purposes:

- **Research**: Access to health data enables studies on public health, the development of new treatments, and the identification of disease trends.
- **Health Monitoring and Planning**: Authorities use data to monitor population health, plan health services, and create public health initiatives.
- **Quality Assurance**: Health data can be used to evaluate the quality of healthcare services, for instance, by measuring treatment outcomes.

Security and Privacy

All processes related to the secondary use of health data must ensure privacy protection. The next two sections describe those processes.

Strict procedures for access control and data handling

Requirements for regulatory and legally mandated consent, or exemptions from consent requirements for some research projects.
Continuous evaluation and compliance with GDPR and national laws.
By facilitating safe and effective use of health data for secondary purposes, this system helps strengthen healthcare services, support research, and improve public health in Norway.

In Norway, presently there is no mutual or one common secure transport infrastructure for health data intended for secondary purposes.

NorTRE (Norwegian Trusted Research Environments) is a collaboration between three main institutional research infrastructures for sensitive data in Norway: HUNT Cloud at NTNU, Services for Sensitive Data (TSD) at UiO, and SAFE at UiB. NorTRE shares knowledge and expertise to enable the collection, analysis, storage, and sharing of sensitive data in an optimal and reliable manner.

Concrete examples of how data is actually shared include:

- **Uninett FileSender**: A service that allows users to upload and share large files securely via email. The service is available to students and staff at Norwegian universities and colleges through Feide login.
- **FOT (Filoverføringstjenesten)**: An infrastructure that supports secure and efficient data transfer between research and educational institutions in

Norway. FOT ensures that data can be transferred quickly and reliably between different entities.

- **Kiste solutions**: This refers to specialized solutions for the secure storage and transport of sensitive data. Examples include the Orbit Nordic kiste, which is designed to be environmentally friendly and sustainable while providing secure storage and transport of data.

The following key elements for common transport infrastructure are missing in Norway:

Secure transport Channels: There is no unified infrastructure that utilizes secure, encrypted communication channels for transferring health data, which would protect the data from unauthorized access during transmission.

- **Logging and Access Control**: There is no unified infrastructure with functionality for logging and monitoring activities related to the data.
- **Compliance with Legal Requirements**: There is no unified infrastructure designed to adhere to national and European privacy regulations, including GDPR, the Health Register Act, and the Personal Data Act, ensuring that all secondary users of health data comply with strict security and privacy requirements.

There are currently no approved Secure Processing Environments (SPE) in Norway.

- Some research institutions and universities have developed their own certified secure processing environments to handle sensitive health data in compliance with national regulations and GDPR. These environments offer secure storage and analysis tools and are only accessible for approved projects with strict access and security controls.
- Several of the research environments collaborate with us in the SPUHIN project to uncover requirements for SPE's in connection with the EHDS regulation, and how to meet these requirements, and how to meet these requirements. You can read more about this here.

Manual work

At present, there is a substantial amount of manual work involved in the processes necessary to support secondary use of health data in Norway. The amount of such manual work and within which data management process it is found varies across the health registers. Health research projects and other secondary purposes, such as quality improvement and health service planning, often require data from multiple

health registries and other sources, which involves numerous manual processes. Here are some key areas where manual work occurs:

Data Collection from Various Registries

Health data in Norway is often fragmented and stored across different national registries. Extracting and combining data from multiple registries often requires manual coordination and communication between registry administrators and researchers.

Data Preparation and Quality Assurance

Once data is collected by the HDAB, it often needs to be prepared and adapted for specific research needs. This includes data anonymization, pseudonymization, and adjustments to ensure data can be analysed in a way that maintains both privacy and research quality. These processes demand significant manual effort from data managers and researchers.

Access Management and Security Measures

Given the sensitive nature of the data, comprehensive security procedures are required, including manual oversight of access control and activity logging. This ensures that only authorized individuals have access to the data and that all usage complies with regulatory standards.

Lack of Automated Solutions

Currently, there are few automated solutions for the secondary use of health data in Norway, meaning some processes such as data collection, integration, and approval procedures, are performed partly manually.

Standardisation

At present, each organization is responsible for managing both standardisation processes and adherence to the European Interoperability Framework (EIF).

Helsedirektoratet NIPH Co-funded by the European Union

Chapter 4

Identified GAPs

Chapter 4

4. Identified GAPs

Identified GAPs are grouped into four areas. These four areas or roles are evaluated based on the difference between the current situation and the desired situation.

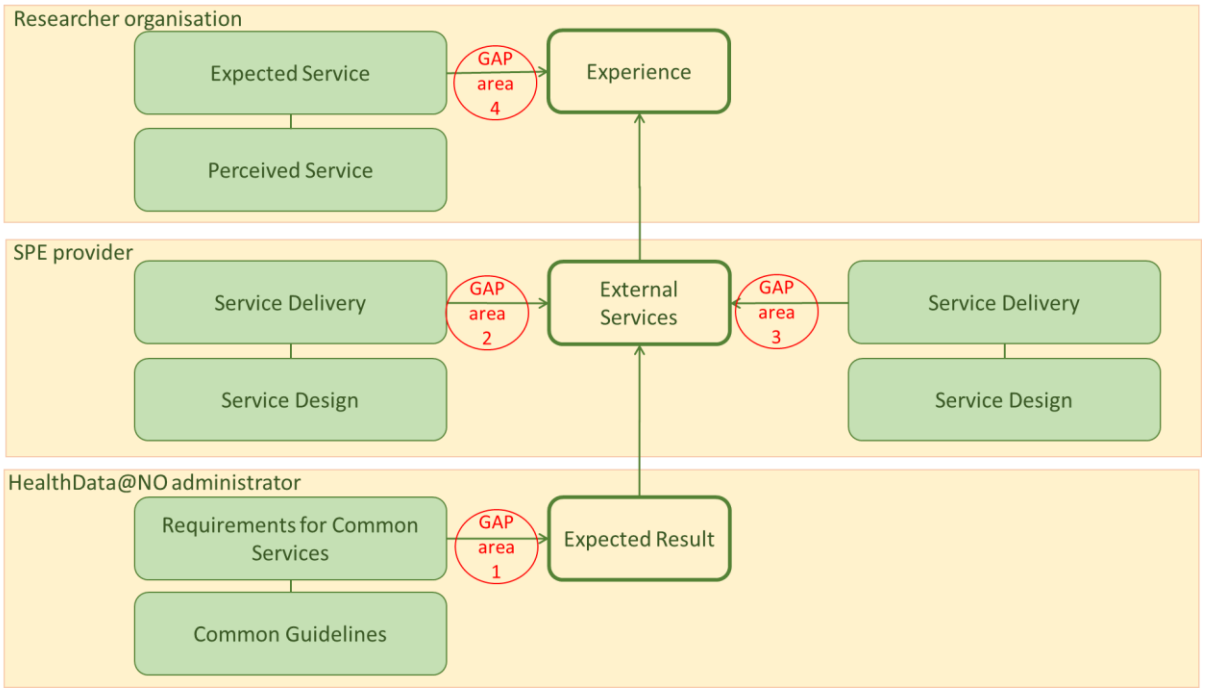


Figure 5 Roles and GAP-areas overview

Each of the four roles, HealthData@NO Administrator, Secure Processing Environment-provider, Data Holder, and Researcher organisation, are in the following analysed for GAP in sub chapters.

To present this in a distinct style, we use codes representing three colours for the capabilities: green indicating good, yellow as ok, and red as not ok. This is shown in figure 3.

Figure 6 : Colours of capabilities status

Here are presented a collection of all the capabilities in this GAP-analysis.

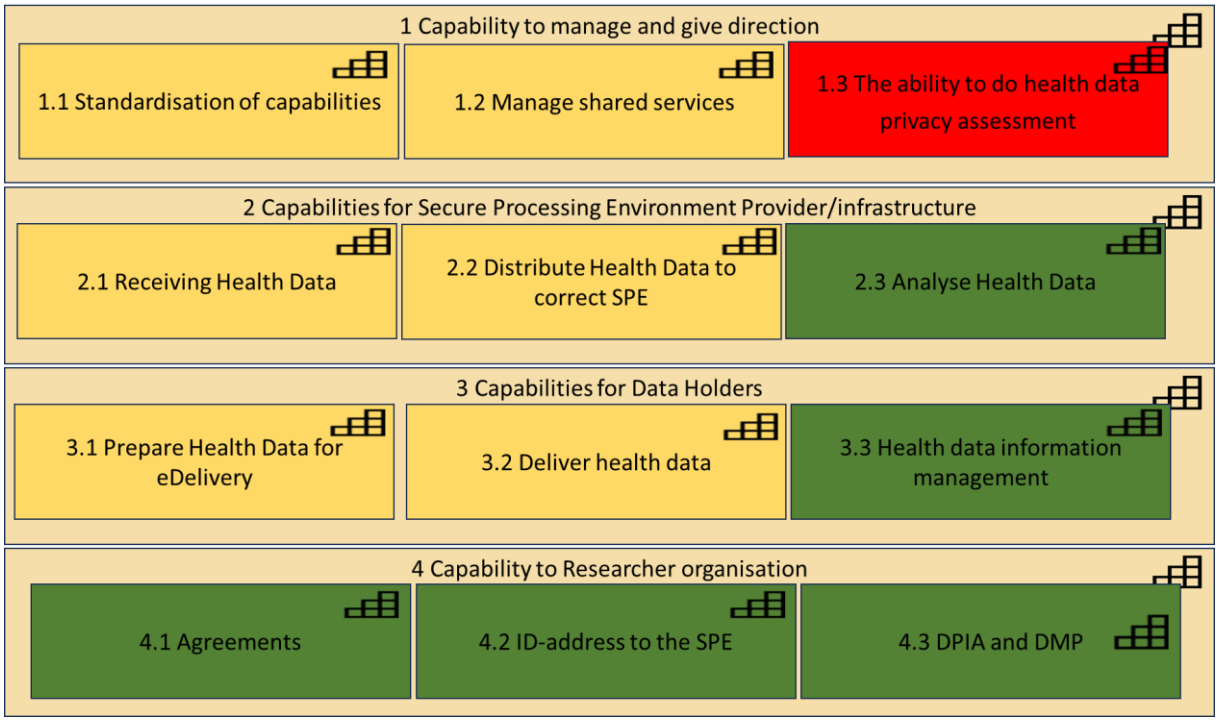


Figure 7 Collection of all capabilities and sub-capabilities in this GAP-analysis

4.1 HealthData@NO Administrator

Capabilities to manage and give direction (GAP area 1)

The role of HealthData@NO Administrator offers capabilities to manage and give direction (1). This will introduce a framework agreement through a structure that makes it easier for various healthcare organizations, socioeconomic registers, and Secure Processing Environments (SPE) to implement and use electronic communication.

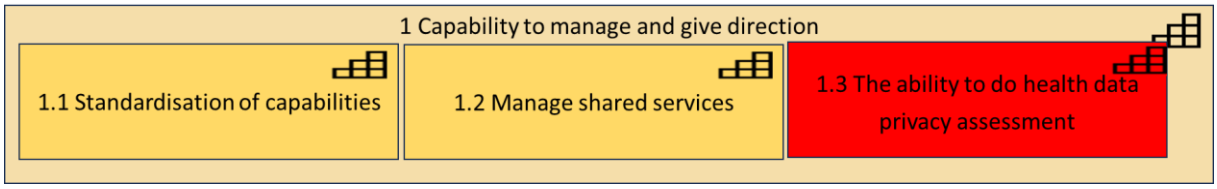


Figure 8 : The capabilities by the Health@NO

Here are the key components of how the HealthData@NO Administrator framework agreement will work:

Agreement for Participation in the HealthData@NO - network

- The **HealthData@NO Agreement** is a collection of standards and guidelines that organizations should follow to participate in the national HealthData@NO network. This includes technical specifications, security requirements, interoperability, and approval for participation.
- The agreement defines how actors, such as public agencies and private businesses, can connect and communicate securely over the HealthData@NO network.

Agreements between HealthData@NO Administrator **and Contact Points**

- A **Contact Point (CP)** is a service provider that connects an organization to the HealthData@NO network. These Contact Points must enter into agreements with **Premiss Giver** to ensure they follow the necessary standards for communication and data exchange.
- HealthData@NO Administrator will establish agreements with Contact Points to ensure that communication between organizations and systems is secure and compatible with the EHDS regulation.

Security and Privacy

An essential part of the framework agreement is to ensure that all communication taking place through the HealthData@NO Network is secure and in compliance with current privacy laws (such as GDPR). This includes authentication, encryption, and access controls to protect data during transport and processing.

Overall, the HealthData@NO Agreements will be a set of technical, organizational, and legal frameworks that ensures all actors in the network can communicate in a secure, standardized, and interoperable way. It helps organizations, both public and private, simplify the electronic exchange of data, reduce costs, and improve efficiency.

Standardisation of capabilities

Capabilities for standardization of secure transport infrastructure (1.1) are essential to ensure that data can be transferred safely and efficiently between systems, especially when dealing with sensitive information such as health data. Here are some key capabilities that must be addressed for secure transport infrastructure:

Security Requirements Capability

This capability defines the security requirements for data transfer, including:

- Encryption, Authentication and Authorization, Integrity

Open Standards Capability

To ensure interoperability and compatibility across different systems and platforms, it is important to use common vocabularies and open standards for data transfer, which may include:

- XML and JSON
- Transport Layer Security (TLS)
- Standard Business Document Header (SBDH)

Technical Infrastructure Capabilities

- Transport Protocols
- Contact Points

Testing and Certification Capabilities

- Testing
- Certification and approval

Interoperability between Systems Capability

- **Standardize interfaces and communication** between different systems to enable secure and reliable data exchange. This can be achieved by using interoperable solutions and secure APIs that support authentication and encryption.

Manage shared services

Managing shared services (1.2) in HealthData@NO Network involves implementing and coordinating shared infrastructure and standards to enable seamless, secure, and interoperable electronic data exchange among multiple parties.

Establish Interoperability Framework

HealthData@NO Administrator manages its shared services through a interoperability framework that ensures compliance with agreed-upon rules, standards, and best practices.

Centralized Components of Shared Services

Shared services include centralized components that ensure interoperability, security, and consistency:

ELMA or Service Metadata Publisher (SMP): A centralized service in Norway that allows participants to register their capabilities (e.g., supported data types and protocols). SMP enables efficient routing and service discovery.

The services ensure that messages are routed to the correct recipients in a secure and standardized manner.

Monitoring and Quality Assurance

Shared services are monitored to maintain reliability and performance. Key aspects include:

Performance Metrics: Regular tracking of service uptime, latency, and throughput to ensure high availability.

Logging and Tracking: Comprehensive logs ensure traceability of message flows and help resolve disputes or technical issues.

Auditing: Periodic audits are conducted to ensure compliance with HealthData@NO agreements and standards.

Ensuring Security

Security is a key priority in managing shared services:

Encryption and Digital Signatures: Ensures data confidentiality and integrity during transmission.

Authentication and Authorization: Secure Contact Points and SMPs use digital certificates to verify identities and access control.
Compliance with GDPR: Ensures proper handling of sensitive data according to European privacy regulations.

Continuous Improvement

Shared services in HealthData@NO Network will evolve over time to meet emerging needs:
Standard Updates: eDelivery protocols are updated to accommodate new use cases or improve efficiency.
Community Collaboration: Feedback from the HealthData@NO -network users will help to refine and expand services.

The ability to do health data privacy assessment

Capability for the ability to do health data privacy assessment (1.3).

HealthData@NO can enhance its ability to perform health data privacy assessments by leveraging the Interoperability frameworks and adapting them to address the unique privacy, security, and regulatory requirements associated with health data.

HealthData@NO will:

Leverage eDelivery Framework for Privacy Protections

The **eDelivery Interoperability Framework**, which ensures secure and interoperable data exchange, can be adapted for privacy assessments:

- **Encryption:** Ensure all health data exchanged is encrypted both in transit and at rest, protecting data from unauthorized access.
- **Digital Signatures:** Authenticate the sender and recipient, ensuring the data's origin and integrity.
- **Access Control:** Define and enforce strict access policies to ensure only authorized entities can access sensitive health data.

Use Logging and Auditing for Privacy Monitoring

The **logging and tracking capabilities** in HealthData@NO -network can be extended for privacy monitoring:

- **Audit Trails:** Maintain detailed logs of who accessed health data, when, and for what purpose to ensure accountability.

- **Monitoring Tools:** Identify and report anomalies or unauthorized data access in real-time.
- **Breach Reporting:** Automate notification of breaches to stakeholders and regulators as required by GDPR and other laws.

Continuous Improvement and Adaptation

- **Feedback Mechanisms:** Collect input from health authorities, service providers, and data subjects to refine privacy assessment capabilities.
- **Adapt to New Regulations:** Update tools and frameworks to align with emerging regulations like EHDS and advancements in health data standards.

4.2 Secure Processing Environment -provider

Capabilities for Secure Processing Environment (GAP area 2)

The role of Secure Processing Environment-provider will offer capabilities (and the infrastructure) for Secure Processing Environment (2) and hold sub-capabilities as Receiving Health Data (2.1), Distribute Health Data (2.2) and Analyse Health Data (2.3).

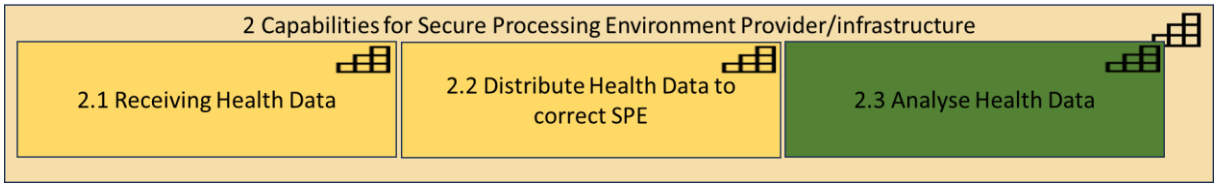


Figure 9: the capabilities by the Secure Processing Environment-provider

Receiving Health Data

The capability Receiving Health Data (2.1) capabilities are to be able to "receive distributions of datasets" containing Health Data by utilizing the eDelivery technology and infrastructure and to validate the delivery. This capability (2.1) is comprised of two sub capabilities that both must be present, and these sub capabilities Connection to eDelivery network (2.1.1) and Validate delivery (2.1.2) are interdependent. These capabilities for Receiving Health Data (2.1) are either mostly manual work or not implemented yet, and hence the status of these sub-capabilities is evaluated as red.

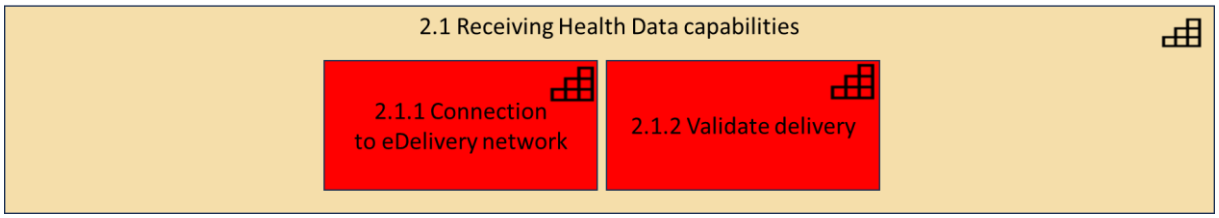


Figure 10 : the sub-capabilities of Receiving Health Data

Connection to eDelivery network

The sub capability Connection to eDelivery network (2.1.1) as the name states are the capability to be able to connect to the network part of the eDelivery and presently limited to the Norwegian eDelivery infrastructure. This connection relies on an agreement between the parties and access to common eDelivery infrastructure.

Validate delivery

The sub capability of Validate delivery (2.1.2) as the name states are the capability to be able to validate the received data over det eDelivery infrastructure. This includes parsing of the delivery and checks for proper format of the eDelivery package, header (SBDH) and body. This validation includes among other confirming the sender and receiver (via ELMA). Also validating or tests for all or most of the security measurements at this stage like the proper use of cryptography, digital signatures, hash, checksums and, fingerprints to mention a few.

Distribute Health Data

The capability by the SPE-P to Distribute Health Data (2.2) to correct SPE or the work to receive a dataset with Health data and forward (routing) to the designated SPE-room and be able to decrypt the received data in the SPE-room.
This capability (2.2) is comprised of two sub capabilities that both must be present, and these sub capabilities are independent. These capabilities for Distribute Health Data (2.2) are not implemented yet, and hence the status of these sub-capabilities is evaluated as yellow.

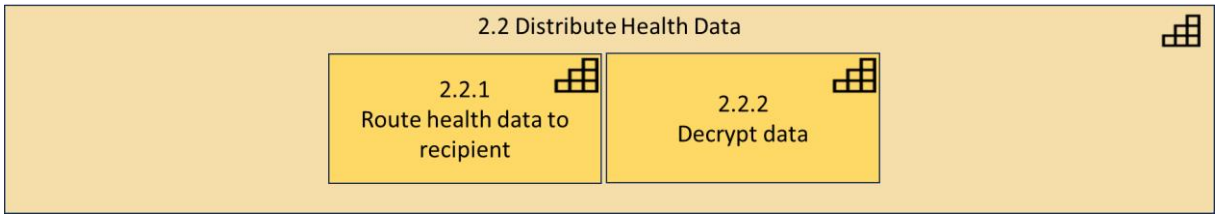


Figure 11: Distribute Health Data

Route health data to recipient

The capability Route health data to recipient (2.2.1) are to be able too forward or to send the secured health dataset to the user in the dedicated SPE-room.

Decrypt data

The capability to Decrypt data (2.2.2) are too be able to decrypt the received (health) dataset within the SPE-room. This will require the knowledge of the decrypting process, information about how it was encrypted or the chosen encrypt algorithm. Additional needed are useful equipment to decrypt and to be able to store the content or the opened data ready for research and analysis.

Analyse Health Data

The capability to Analyse Health Data (2.3) are to be able to provide the receiver, the user, often the researchers with additional tools for analysing the received health information. This is currently working as research is conducting, and for now green.

4.3 Data Holder

Capabilities for Data Holders (GAP area 3)

The role of Data Holder will offer Capabilities for Data Holders (3), and hold sub-capabilities as Prepare Health data for delivery (3.1), Delivery health data (3.2) and Health data information management (3.3).

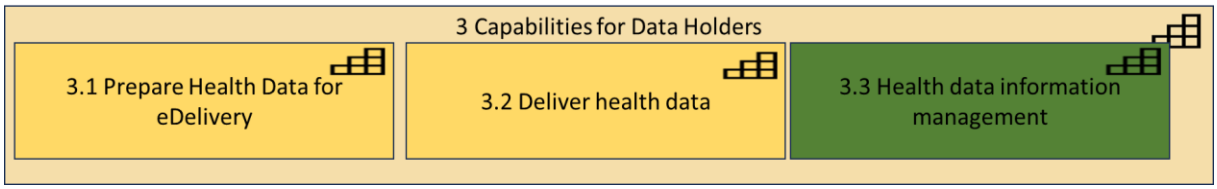


Figure 12: Capabilities for Data Holders

Prepare Health Data for delivery

The capability Prepare Health Data for delivery (3.1) and hold sub-capabilities as are to be able to Produce Datasett (3.1.1), Secure Dataset (3.1.2), Address Dataset (3.1.3).

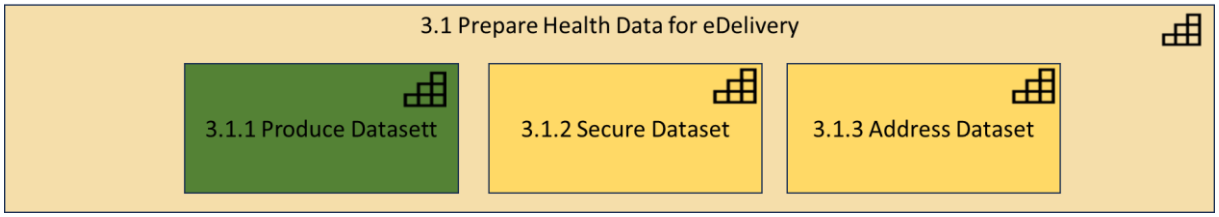


Figure 13: Prepare Dataset for eDelivery

Produce Dataset

Main registries in Norway produces dataset (and distributions) for secondary use and have so for a long time. This has been done through cooperation among registries with respect to Linking, Minimizing, Pseudonymization and Anonymization. In the last couple of years more of this has been coordinated through Norwegian Health data Service (Helsedataservice) which is intended to become the Norwegian HDAB.

Secure Dataset

Disclosure of sensitive health data in Norway takes place and must take place in accordance with current regulations such as cf. the Health Register Act and GDPR . This means that the data must be encrypted with secure encryption, and passwords must not be transmitted in the same channels as the data. For the transport of

sensitive health data, dedicated channels are used. However, encryption is a manual process and can vary between the different health registries.

Address Dataset

There is no common system to ensure datasets are delivered to the right (approved) data user. There are however used a common system for data transport (Filoverføringstjenesten) that helps addressing the right receiver.
The different SPEs have their own solution for safe transport of sensitive datasets into the different project rooms, usually solved by downloading the data from a safe staging area into the project room by an authenticated and authorised project owner.

Deliver health data

The capability Deliver health data (3.2) are to be able to deliver health data through an eDelivery instance.

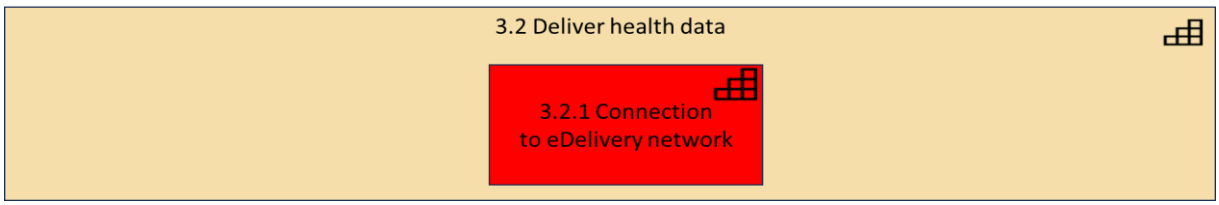


Figure 14 : Deliver health data

Connection to eDelivery network

There is no connection to the eDelivery network (3.1.1) for health data today. However, Norway is closely monitoring developments in the EHDS and is analysing the consequences of the introduction of eDelivery for the exchange of health data for secondary use.

Health data information management

The Norwegian Directorate of Health, the Directorate of eHealth and other health authorities work together to ensure that health information is handled in a safe and efficient manner. This includes the development of national guidelines and standards for the use of health data. At least the Central health registries and National Medical Quality Registries has an extensive data information management have an extended quality control and follow-up of data that comes into the registers.
These registries report their metadata to a common master application for health metadata according to the National specification for health data metadata where they are published to users via the health data site helsedata.no.

4.4 Researcher organisation

Capability to Researcher organisation (GAP area 4)

The role of Researcher organisation will offer Capability to Researcher organisation (4) and hold sub-capabilities of managing Agreements with SPE Provider organisation (4.1), the capability of managing ID-address to the SPE (4.2) and the capability to conduct and manage Data Protection Impact Assessments (DPIA) and Data management plans (DMP) (4.3).

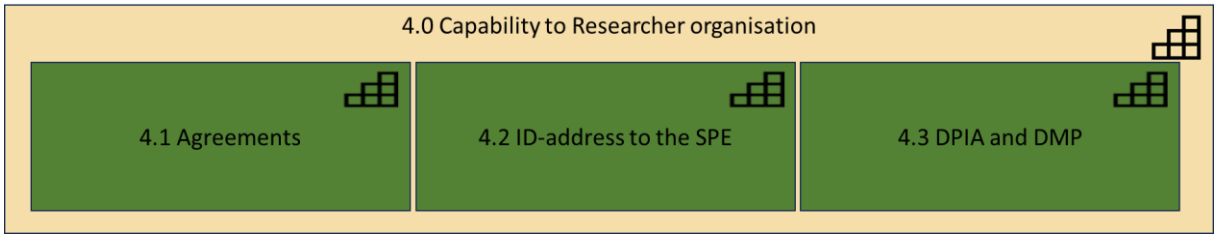


Figure 15: Capability to Researcher organisation

Agreement with SPE Provider organisation

The capability to manage Agreements (4.1) with SPE Provider organisation are to be able to compose, negotiate and comply with agreements, primary with the Secure Processing Environment-Provider. Most of the current parties are evaluated to currently to hold reasonable abilities and capacity for handling Agreements for Participation in the HealthData@NO -network. So, the (4.1) GAP is green.

ID-address to the SPE

The capability to manage the ID address of the SPE (4.2) operates on two levels.
1) The first level is the ID of the SPE provider used by the researcher for their research, and the 2) second level is an ID directly linked to the SPE where the research will be conducted. It is essential that this ID accompanies the application for access to the health data and any other data being applied for.
The SPE Provider's Contact Point specifies the ID used by the SPE provider in the Service Metadata Publisher (SMP), which in Norway is called ELMA. This ID should correspond to the organization number of the SPE user organization. In the application for health data and any other data, the SPE user organization must be included.

This point is considered a capability that is currently satisfied (Green).

Data Protection Impact Assessment and Data Management Plan

The capability to conduct and manage Data Protection Impact Assessment (DPIA) and Data management plan (DMP) (4.3) for the Researcher organisation are to be able to do a continually improvement process and data linage evaluation of the research conducted. This work is essential for the trustworthiness of the Researcher organisation and the research conducted. The current parties are evaluated to currently to hold reasonable abilities and capacity to conduct and manage DPIA and DMP.

Helsedirektoratet

NIPH

Co-funded by the European Union

Chapter 5

Bridge from the current, towards the desired state

5. Bridge from the current, towards the desired state

The main task for secure transport of health data in Norway is to implement the HealthData@NO network, which is based on eDelivery, a technical infrastructure and a set of standards developed by the EU to enable secure and reliable electronic data exchange between public authorities, private businesses, and other organizations in Europe.

The main purpose of eDelivery is to support electronic communication and ensure that data can be safely transferred between different parties, especially when it comes to sensitive or confidential information, such as health data or legal documents.

The HealthData@NO network is a national network for the exchange of health data for secondary use, which can be utilized by businesses that gain access to the network. The national network also has the capability to send and receive data from the EU Commission's central service for secondary use and other member states that join eDelivery. The HealthData@NO network connects all members in a secure and interoperable manner, as long as they use a standard Contact Point. Members that can join the network include:

- National medical quality registers
- Biobanks
- EHR providers
- Regional Health Authorities (RHAs)
- Socioeconomic registers
- SPE (Secure Process Environments)
- HDAB NIPH

Furthermore, HDAB NIPH is connected to the National Contact Point, which is a Cross-Border Contact Point. This Contact Point has access to exchanges within HealthData@EU, reaching EU member states and The EU's central service.

Standard Business document Header

The standardised format of the Standard Business document Header (SBDH) adds important information about the health data for secondary use, such as who sent it, who receives it, what type of data it is, and when it was sent. This helps to automate and streamline document handling.

Structure: SBDH consists of several elements, including:

`HeaderVersion``: The version of the SBDH standard being used.`
`Sender``: Information about the sender of the document.`
`Receiver``: Information about the receiver of the document.`
`DocumentIdentification``: Unique identification for the health data.`
`BusinessScope``: Details about the business process the document is part of.`

By using SBDH, we expect to reduce manual handling of health data, minimize errors, and improve traceability and security in document exchange.

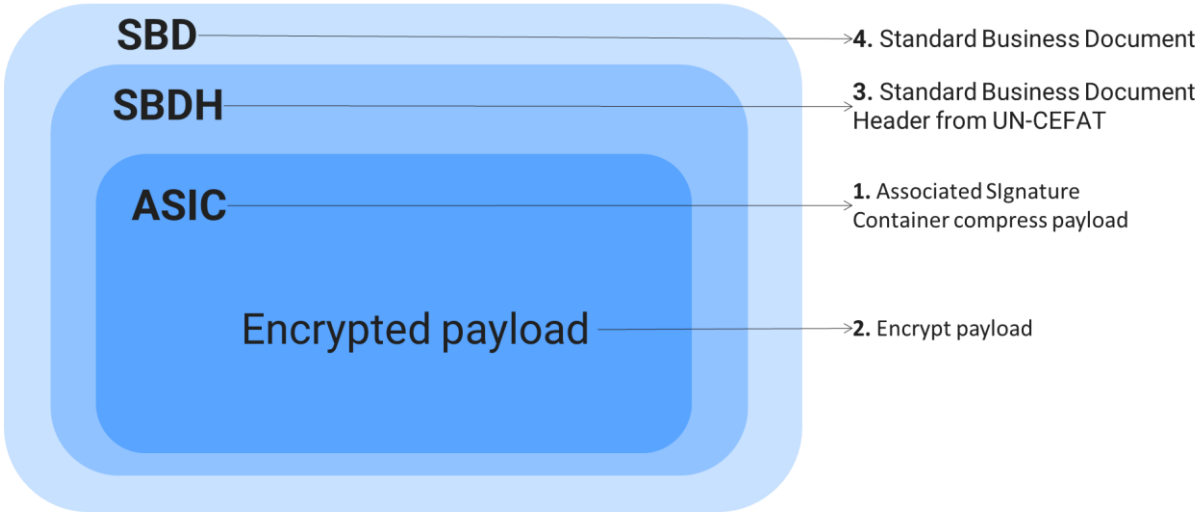


Figure 16: Standard Business Document structure

Associated Signature Containers ASIC

Associated Signature Containers – Extended (ASiC-E) is a file format standardized by European Telecommunications Standards Institute (ETSI) for packaging data of various types. This container can hold one or more signatures. Each file object can include payload, additional information, or metadata that can be protected by the signature.

The approach to securing health data for secondary use involves first creating an ASiC-E archive and then encrypting this archive. This method leverages the compression efficiency of the ASiC-E format for both the payload and attachments.

Encrypting documents prior to compression significantly reduces the achievable compression rate, making this two-step process more efficient.

5.1 Action plan

Carry on the EHDS Pilot Proof of Concept

Nationally, we will target the establishment an HealthData@NO Network based on eDelivery, and the work conducted in the SPUHiN - EHDS Pilot Proof of Concept (PoC).

Additional security measures will be identified and introduced, including:

- **Certificate issuing**: All Contact Points and Access Points will need to be issued certificates that are part of a certificate chain, ensuring that only pre-approved participants can join the network.
- **Ensurance of identity and confidentiality**: End-to-end encryption of content will need to be implemented, based on the recipient's public encryption certificate, and the content will be signed to verify whether it has been altered.
- **Capability determination**: The solution will need to leverage a Capability Look-up capability, using e.g., a national Service Metadata Publisher (SMP) called ELMA.
- **Interoperability Framework definition and establishment**: An Interoperability Framework will need to be established to define how the national network will function, including technical specifications.

Cross Border solution

The National HDAB will focus on implementing the eDelivery solution developed by the EHDS Pilot during the Connectathon in 2025.

5.2 How to follow up the Action Plan

Complete the Proof of Concept

The Proof of Concept effort will be completed by January 2025. By the end, we will have several learning points that will be addressed in the subsequent work.

Continuously assess compliance with the EHDS regulation

The National HADB responsible for the cross-border Contact Point will monitor developments in the EHDS and always remain compliant with the regulations.

Establish the role of HealthData@NO Administrator

The work to establish an HealthData@NO Administrator will begin in 2025, focusing on creating an HealthData@NO Interoperability Framework. This framework will evolve over time based on experiences and feedback received. Additionally, we will review the work done in OpenPEPPOL and incorporate some of the lessons learned from their efforts.

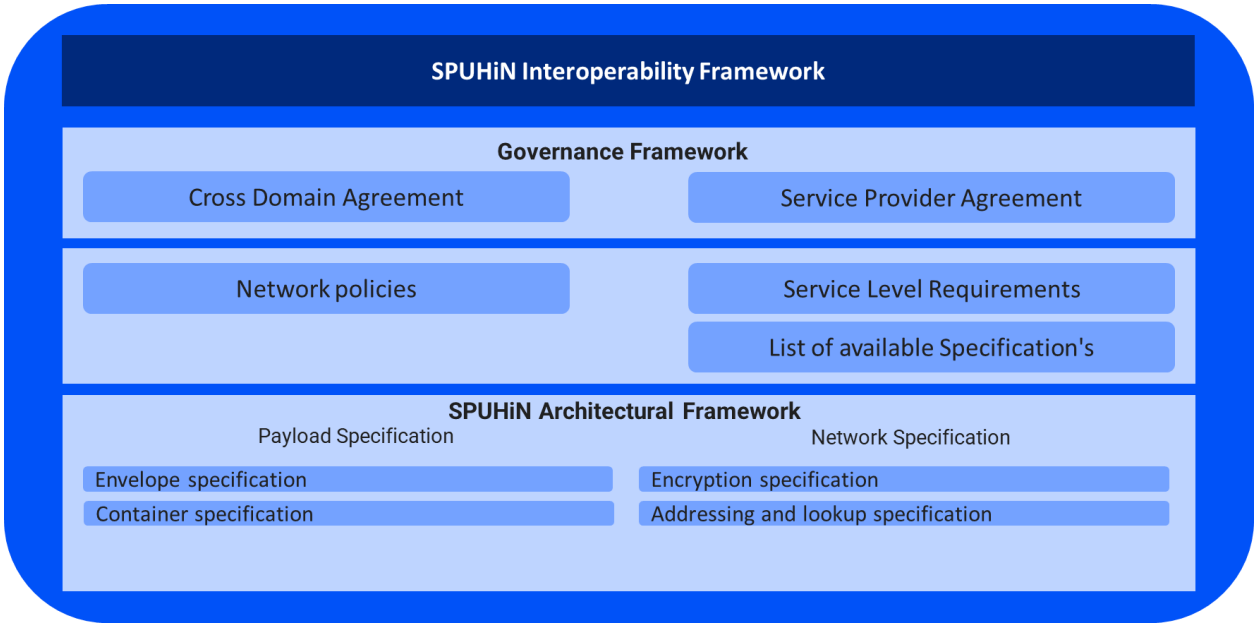


Figure 17: The SPUHiN interoperability framework

Project number: 101128232
Milestone: D8.2
Date: 28.11.2024