Co-funded by the European Union

FAIR Secure Procurement and Use of Health data in Norway (SPUHiN)

Recommendations for minimum requirements for Secure Processing Environments in Norway

Project number: 101128232

Milestone: M10

Date: dd.mm.yyy

Disclaimer: "Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them."

Content

Background

As part of the European Health Data Space (EHDS) regulation there will be requirements to use Secure Processing Environments (SPEs) for processing of health data for secondary purposes. In Norway, it is mainly the responsibility of the applicants of health data, as data controllers according to GDPR, to determine where such analysis is to be performed. The data controller must ensure that the health data is sufficiently protected after it has been provided by the data holders. The Norwegian regulation on a national solution for access to health data points to use of a "closed and secure analysis infrastructure"[1]. There is however no further definition or specification of the concept closed and secure analysis infrastructure, and the Norwegian regulation also states that access can be provided in other ways if it is deemed necessary.

Based on the descriptions provided by the applicants in their permit application to Health Data Service (the national Health Data Access Body, HDAB) for personally identifiable health data during 2023, there is a large variety on how data will be stored and processed. It is however most common to use either an analysis infrastructure currently available from the universities, see table 1 below, or some type of server, database, folder, area or zone most likely provided by the data controller's own IT provider. A few also refer to OneDrive, Office365, disconnected PC or a partner in another country.

Before further guidance and implementing acts on SPEs are available from the EU, a set of recommended minimum requirements for SPEs have been developed in Norway to prepare SPE providers to comply with future EHDS regulation. These recommendations are also intended to help permit applicants, Health Data Service (HDAB) and other stakeholders to harmonise the understanding of what may be defined as a "closed and secure analysis infrastructure".

The recommendations in this document are a product of the project FAIR Secure Provision and Use of Health data in Norway (SPUHiN) that is partly funded by the EU and a collaboration between the Norwegian Directorate of Health and the Norwegian Institute of Public Health. The most commonly used analysis infrastructures have also been important participants in the project, namely:

Service	Description	Organisation
TSD	Services for Sensitive Data	University in Oslo (UiO)

[1] Forskrift om nasjonal løsning for tilgjengeliggjøring av helsedata - Lovdata

SAFE	Secure access to research data and e-infrastructure	University of Bergen (UiB)
HUNT Cloud	Research infrastructure for researchers working with sensitive data	Norwegian University of Science and Technology (NTNU)

Table 1, The providers of analysis infrastructures from the universities.

The above providers of analysis infrastructures, have all been part of a gap-analysis[2] that has been used as a basis for further development of the recommendations in this report. A broad range of other stakeholders have also been involved in providing input to these recommendations, mainly through a series of workshops in Q2 of 2024 and an informal hearing in Q1 2025. The stakeholders involved include users of health data (including researchers and public/private sector), Health registries, SPEs (including at universities and hospitals, private/public sector), Authorities (including Data protection, Directorates in digitalisation and knowledge) and Experts in security, architecture, legal, privacy and standardisation.

These minimum requirements will contribute to the definition of what can be considered an SPE in Norway. The objective is also to increase security and control over health data that is granted use for secondary purposes and prepare for the implementation of EHDS requirements through stimulating increased use and development of SPEs.

Definitions

Definition of	**Description**
SPE	Secure Processing Environment. The dedicated environment / space where the user of health data performs their analysis. An SPE is a technical instance of the SPE infrastructure.
SPE infrastructure	The total of the technical environment at the SPE provider that is necessary to provide several user instances of SPE's.
SPE owner	The person legally responsible for the use of the SPE. This is typically a project manager, Principal Investigator (PI) or similar that is responsible for the research project and is the responsible for the data permit. Responsibilities of an SPE owner can often be formally delegated.
SPE provider	The organisational unit that operates and maintains the SPE infrastructure.

[2] SPUHiN D5.1 Gap analysis report – SPE requirements – feb 2024.pdf

SPE provider organisation / Organisation of the SPE provider	The organisation of the SPE provider. For smaller organisations this may be the same as the SPE provider.
SPE user	The persons that log on to an SPE to perform analysis or administration of their dedicated SPE.
SPE user organisation / Organisation of the SPE user	The organisation that is responsible for the project or research unit that is using the SPE.

Table 2. Definitions

Scope

The checklists below are developed as a recommendation for minimum requirements for use of Secure Processing Environments (SPE) during storage and processing of health data for secondary purposes following a data permit. The check lists may also be used as guidance for storage and analysis of health data for secondary purposes where the data permit is not issued by HDS.

It is still always the responsibilities of data controllers and data processors according to GDPR that should the basis for any assessments regarding use of SPEs.

The check list for SPE providers also provide a basis for self-assessment of compliance. Self-assessment of compliance from SPE providers may help data controllers in their assessment of which services that may provide a sufficient protection for the health data they are processing for secondary use.

The recommendations described in this document are based on the assumption that a copy of health data according to the permit is transferred from the data holder to a destination determined by the permit holder. If solutions that allow federated analysis become more commonplace, there may be need to revise these recommendations.

The recommendations are also based on the current architecture for the services provided by the major analysis infrastructures that are most commonly used today (see table 1). These services typically provide a digital interface to a virtual desktop workspace with the possibility to both store large amounts of data and access different tools to analyse and work with the data.

The scope and requirements will need to be updated when further guidance and implementing acts for Secure Processing Environments are available in the EU.

Check list for SPE providers

This chapter contains a check list of requirements that are recommended to be in place for SPE providers. The recommendations are intended to be a help for several different actors, including:

- SPE providers when developing their SPE services and presenting their level of compliance through self-assessment.
- SPE user organisations when assessing the use of SPE providers as part of their data controller responsibilities.
- Health Data Access Bodies (such as Health Data Services) when providing guidance regarding use of SPEs and as input in the permit application process.

It is important to point out that the requirements in the SPE provider checklist consist of activities and functionality that the SPE provider can be considered to be responsible for in their role as data processor. Most of the requirements are there to make it easier for the SPE user organisation to be able to succeed in their responsibilities as data controller through providing necessary functionality.

A number of requirements in the SPE provider check list are expected to be complemented by activities performed at the SPE user organisation. Documenting the complementary requirements in the check list for SPE user organisations (see next chapter) is intended to provide a clear division of responsibility between the SPE user organisation and SPE provider.

The set of recommended requirements will be an important part in reaching a common understanding of what can be considered an SPE in Norway and a closed and secure analysis infrastructure. Increased use and development of SPEs in the direction of the recommended requirements will also contribute to increasing security and control over health data that is granted use for secondary purposes and prepare for the implementation of EHDS requirements[3].

Below is a description of the different columns in the check list table.

- **Nr** – Enumeration of the requirements for easier reference. Starts with a P for Provider.
- **Area** – Grouping of the requirements for easier reference.
- **Requirement (with title)** – Description of the requirement. Includes a title for easier reference.

[3] See mapping in (Attachment) Relation to EHDS, Article 73 – Secure Processing Environment

- **Comment/Guidance/Rationale** – Description intended to explain the reason why the requirement is included in the check list and point out specific circumstances that may be relevant for the requirement. This includes relation to specific requirements in the SPE user organisation check list.
- **Importance** – These are recommendations on how important it is that the requirements are in place at the SPE.
  - Mandatory – Recommended to be set as a mandatory requirement to an SPE provider, e.g. by an SPE user organisation when acquiring an SPE service from an SPE provider. It is recommended that acceptance of any deviations, with or without compensating controls, is assessed, and documented.
  - Recommended – Recommended to be set as recommended requirement to an SPE provider. Several recommended requirements are potentially to be expected when EHDS is implemented but the necessary functionality may not yet be available.
- **Examples of implementation** – Description of examples of different alternatives of how a requirement can be implemented, or different activities/functionality that may be relevant for implementation.

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
P1	ISMS	**Information security management System (ISMS)** The organisation of the SPE provider must have an operating information security management system (ISMS) according to the requirements in ISO/IEC 27001.	To have an ISMS in place is already a requirement from other laws (including GDPR). An explicit reference to the requirements in ISO27001 has been assessed beneficial for several reasons, such as harmonisation, clear expectations, common language, possibility for certification.	Mandatory	• The ISMS of the SPE provider follows ISO27001. • The ISMS of the SPE provider follows the NIST Cybersecurity Framework (CSF) but there is a mapping to the requirements in ISO27001 and they are covered.
P2	ISMS	**ISMS scope** The scope of the ISMS must cover the SPE provider's organisational units, locations, and processes for providing the SPE infrastructure.	It is important to ensure that the ISMS at the SPE provider is valid for operations of the SPE infrastructure.	Mandatory	• Policy documents show that there is a clear connection between with the overall ISMS of the SPE provider organisation and the ISMS-related activities performed for the SPE infrastructure.

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
					- The ISO27001 certificate proclaim that the SPE infrastructure is in scope.
P3	ISMS	**ISMS certification** It is recommended that the SPE provider is ISO27001 certified.	An ISO27001 certification can provide assurance that the ISMS at the SPE provider is operating.	Recommended	- The SPE provider is ISO27001 certified according to the established international certification scheme.
P4	Access	**Identification level** All users that can provide an eID identified with a high level of assurance according to eIDAS[4] must be required to log in to the SPE using such an eID. The SPE provider must only allow access to other users if the identity of the user has been verified by the SPE user organisation.	An important part of having control over the data in the SPE is to be able to verify that the persons that gain access are who they claim to be. However, there are no fully available technical solutions for eIDAS level high that provide access to SPE users who are not residents of Norway. An increased focus on personnel security requirements is anticipated, following the proposed changes to Norwegian regulations that would permit background checks for personnel in critical positions with access to large health data sets[5]. For users without the necessary eID assurance level, the **SPE user organisation requirement "U2 – Manual identification"** must be in place to complement this SPE provider requirement.	Mandatory	- Identification with BankID is required when logging into the SPE. Verification of possession of a valid passport or national ID-card through the bank's "Know your customer"-procedures is required before a bank can issue a BankID. - When onboarding a new SPE user that does not have BankID, the SPE provider requires that the SPE user organisation has verified the identity of the SPE user, e.g. through verification of a valid passport. The SPE provider require assurance that the identity of the SPE user has been verified via, e.g.: ○ a mandatory checkbox in the form that SPE owners need to fill in when creating new users without BankID, or ○ an e-mail from the SPE user organisation stating that verification has been done.
P5	Access	**Verification of organisation affiliation**	This is one of several controls that contribute to ensure the SPE user	Recommended	- For registration of user accounts in the SPE, only e-mail addresses from

[4] Article 8, §2c https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910
[5] Høring - krav om bakgrunnssjekk - regjeringen.no

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
		It is recommended that the SPE provider provides login solutions that verify the SPE user works at the organisation they claim to represent.	has a valid reason to have access to the data. Technical solutions do not yet have full support for this, but manual procedures may be used.		the research institution affiliated to the project are accepted. • The user eID has a property that link the user to their employer organisation, and this property is checked at login to the SPE. (This functionality may be possible to implement with eIDAS 2.0).
P6	Access	**Multi-factor authentication** Multi-factor authentication must be required to log in to an SPE.	Due to the weaknesses with using only userID and password, this requirement is important enough to specify as a minimum although it is expected for services holding sensitive data.	Mandatory	• SPE users need to approve log in through a BankID app on their mobile phone. • SPE users need to approve login by providing a onetime code sent via SMS to their mobile phone. • The SPE use a multi-factor authentication solution that is phishing resistant.
P7	Access	**Access approval** The SPE provider must have formal procedures in place to ensuring only SPE users that are approved by the SPE owner are provided access to the SPE.	Access approval procedures at the SPE user organisation may be circumvented if the SPE provider does not verify that an access request is made by an authorised individual (such as SPE owner) prior to providing the requested access. **SPE user organisation requirement "U4 – Access approval"** must be in place to complement this SPE provider requirement.	Mandatory	• The SPE has a self-service function where only the SPE owner can grant access rights to the SPE. An identifiable log of granted access is retained. • SPE provider staff must only act on manual access request from the SPE owner or a person from a list of defined delegates. Evidence of approval of access is retained.
P8	Access	**Removing access** The SPE provider must provide functionality or services to the SPE owner to ensure that access is removed for SPE users that no longer shall have access to the SPE.	Access termination procedures at the SPE user organisation may be difficult to execute if the SPE provider does not implement efficient functionality or services to	Mandatory	• The SPE has a self-service function that allows the SPE owner to easily remove access rights for SPE users. • The SPE provider offers a manual routine for requesting removal of access to the SPE.

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
			ensure that access rights can easily be removed. **SPE user organisation requirement "U5 – Removing access"** must be in place to complement this SPE provider requirement.		
P9	Access	**Access according to data permit** It is recommended that the SPE has technical functionality to ensure that only SPE users included in the valid data permit have access to the SPE.	A direct technical connection between the data permit and access rights is currently not available but may decrease the risk of unauthorised access. This control has the potential to automate a large portion of other access management controls both at the SPE provider and SPE user organisation.	Recommended	• A list of the persons allowed access according to the data permit is provided to the SPE provider and is used as input to a function in the SPE that verifies that only persons in the list have user accounts in the SPE.
P10	Access	**Review of access** The SPE provider must provide functionality to ensure that SPE user access rights are easily available to the SPE owner to perform regular review of access.	Access review procedures at the SPE user organisation may be difficult to execute if the SPE provider does not implement efficient functionality or services to ensure that an overview of access rights is easily accessible for review. **SPE user organisation requirement "U6 – Access review"** must be in place to complement this SPE provider requirement.	Mandatory	• Self-service function for the SPE user organisation to perform review of access rights. Log of the review is retained. • The SPE provider regularly sends a list of current access rights to the SPE owner. • Automatic function for SPE owner to re-approve SPE user access rights e.g. every 6 months or 1 year.
P11	Access	**Restriction of SPE provider access** The SPE provider must limit the number of employees at the SPE provider or sub-contractors that have high privileged access that implies that they can access or acquire access	IT systems are inherently built so that users with high privileged access on an infrastructure level most often can appropriate access to customer data even though this is	Mandatory	• To provide sufficient robustness in the operations of the SPE infrastructure there are 5 from the SPE provider that can log on as administrators when necessary.

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
		to health data in the SPEs in the SPE infrastructure.	not wanted. Limiting the number of users with such access narrows down users to follow up.		
P12	Access	**Access management for SPE provider access** The SPE provider must have effective procedures for access management of employees at the SPE provider or sub-contractors that have high privileged access that implies that they can access or acquire access to health data in the SPEs in the SPE infrastructure.	Robust procedures for access management are expected to be in place in an ISMS for providers of services holding sensitive data. They may however sometimes be complex to accomplish and are important enough to include as a minimum requirement.	Mandatory	• There is a clear definition of which roles in the IT department at the SPE provider organisation that may have the need for administrator access and the corresponding approval procedures. Such administrator access is also defined as a high-risk role in the procedures for personnel security. • The access management procedure for administrators in the IT department at the SPE provider organisation includes requirements for documented manager approval of new users and there are robust procedures to ensure that access is removed when it is no longer necessary. • When a person in the IT department logs on to their approved administrator account the access is logged. They are also prompted to type in the reason for the access, including the relevant service ticket number.
P13	Logging	**Logs of access to SPE** The SPE provider must keep tamper proof and identifiable logs of access to the SPE for at least one year.	The EHDS regulation will require that identifiable logs of access to the SPE are kept for at least one year. One relevant objective for retaining such logs is the possibility to follow up unwanted access which means that	Mandatory	• Logs of access to the SPE include: ○ User identity that accesses the SPE. ○ Date and time for access (clocks are synchronised with approved time sources).

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
			it is important that the logs cannot be tampered with.		○ IP address or other identification of the unit used for access. • Logs of access are sent to a dedicated log server that have functionality to ensure that the integrity of the logs are preserved. • Logs of access are retained for one year.
P14	Logging	**Logs of activities in the SPE** It is recommended for the SPE provider to keep tamper proof and identifiable logs of activities in the SPE.	The EHDS regulation will require that identifiable logs of activities in the SPE is kept, but it has not yet been further defined what is meant by “activities”. What activities that are logged in the SPE should be determined by what the logs are intended to be used for based on relevant risks.	Recommended	• Use of tools and changes to data in the SPE are logged to be able to detect suspicious activities and follow up unwanted incidents. • Read access to the data is logged to be able to detect snooping in an SPE with large amounts of clinical data. Logs are retained until they have been used in the control for snooping that is performed quarterly. • INSERT, UPDATE and DELETE commands are logged in an SPE SQL database to be able to verify the integrity of the data as part of validating the research results. The logs are retained until the analysis results have been verified.
P15	Logging	**Log monitoring** It is recommended that the SPE provider have effective procedures for monitoring and review of logs based on risk.	The need for monitoring and review of logs will differ based on risk and the purpose of logging. It is expected that some level of responsibility of monitoring will lie with the SPE provider, but it is recommended that this is agreed and clearly regulated in agreements with the SPE user organisation.	Recommended	• The SPE has a self-service function for the SPE user organisation to access relevant logs for review. • The SPE provider offers a service where SPE provider monitor logs and report on suspicious activities.

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
P16	Data import	**Encryption during data transit** The SPE provider must provide functionality to make it easy to encrypt the regulated data in line with current strong encryption standards, while in transit between the data holder environment and the verified SPE.	Not all data holders and SPE providers have developed secure services for machine-to-machine data transfer from the data holder systems into any SPE. To protect the health data from unwanted disclosure it is still important that it is encrypted at the data holder and not decrypted until it is imported into the SPE (end-to-end encryption). Although this is largely the responsibility of the data holder and/or the SPE user organisation, it is important that SPE providers develop their SPE services to make end-to-end encryption from the data holder easy.	Mandatory	• The data is transferred directly from the data holder system into the dedicated SPE using a data transport service that supports end-to-end encryption. • The data is encrypted by the data holder on file or database level and the SPE has the necessary tools to decrypt the data after it has been imported into the SPE.
P17	Data import	**Machine-to-machine data transfer** The SPE provider is recommended to provide functionality to make it easy to transfer data digitally from the data holder environment to the verified SPE without manual intervention.	This requirement is currently not mandatory because the required services are not yet available to all. Secure machine-to-machine transfer of health data with strong end-to-end encryption from the data holder systems into the SPE indicated in the data permit should be the preferred option when developing technical solutions for data transfer to SPEs. Although this is also the responsibility of the data holder, it is important that the SPE providers develop their SPE services to allow for machine-to-machine data transfer. End-point termination in	Recommended	• The SPE provider has an access point for eDelivery to allow for secure machine-to-machine transfer from the major health registers with end point termination in the dedicated SPE in the SPE infrastructure. • The SPE provider has a well-documented secure data transfer protocol that can be used to upload data directly from data holder systems into the dedicated SPE.

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
			the SPE is strongly encouraged over termination at the SPE infrastructure. To ensure successful implementation of data transfer solutions it is also important that a broad range of user needs are supported, including large data sets, continuous updates and live queries. Where machine-to-machine data transfer is not in place, the **SPE user organisation requirement "U7 – Register data import"** must be in place to complement this SPE provider requirement.		
P18	Data import	**File import** The SPE must have functionality for the SPE user to import files only in a dedicated and controlled manner.	Technical limitations on how the SPE user can import data narrows down the import points where access to importing files can be controlled and where malware may be introduced. In most practical cases an SPE user will import data in some type of file format. The main principle is that the SPE owner is responsible for managing the risk of importing files into their own SPE. This is based on the fact that incidents inflicted by imported files will not result in leaked health data from the SPE since there are strict controls on file extraction and any outbound connections. In addition, only the SPE where the file was imported will be impacted by	Mandatory	• The SPE user can only import data through a dedicated, controlled and monitored one-way file import function. • Files are checked for virus prior to import into the SPE.

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
			any incidents due to separation of environments.		
P19	File extraction	**Restricted file extraction** The SPE must have functionality for the SPE user to extract files only in a dedicated and controlled manner.	Technical limitations on how data can be extracted from the SPE narrows down the extraction points to control to ensure that only non-personal data is extracted from the SPE. In most practical cases an SPE user will export data in some type of file format.	Mandatory	• SPE users do not have access to the internet from within the SPE. • It is not possible to copy data out of the SPE via the system clipboard. • The SPE user can only extract data through a dedicated, controlled and monitored file export function.
P20	File extraction	**Identification level for roles extracting files** Only SPE users that have been identified with eIDAS level high can be provided access rights to extract files from the SPE.	Persons that have access rights to extract files from the SPE must to some extent be trusted to only extract non-personal data. Therefore, it is important that there is a high level of assurance that such persons are who they claim to be.	Mandatory	• Only users that log on using BankID may be given an access role that can extract files from the SPE.
P21	File extraction	**Role for extracting files** The SPE provider must restrict access rights to extract files (unless the data in the files is certainly non-personal) to a defined high risk access role in the SPE.	A clear definition of which role that can extract files provides a basis for other controls to ensure that only non-personal data is extracted from the SPE. **SPE user organisation requirement "U8 – Limit access to extract files"** must be in place to complement this SPE provider requirement.	Mandatory	• The access rights necessary to extract files from the SPE are technically tied to a standard access role that can be granted to an SPE user. The SPE owner organisation can easily obtain an overview of the SPE users that have this access role. • The SPE provider has a clear description of what access rights that are necessary to extract files from the SPE. Although the access rights are manually configured for each SPE user the SPE owner organisation is able to easily obtain an overview of the SPE users that

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
					have the access rights required to extract files.
P22	File extraction	**Verification of user training on file extraction** Prior to granting access rights for extracting files, the SPE provider must obtain verification from the SPE user organisation that the SPE user has performed training regarding what data that is allowed to extract from an SPE.	Persons that have access to extract files from the SPE must to some extent be trusted to only extract files with non-personal data. Therefore it is important to ensure that such persons know what data is allowed to extract, and how to extract these data from an SPE.	Mandatory	• Prior to granting user access rights to an SPE user account for extracting files, the SPE provider requires that the SPE user organisation verifies that the SPE user has performed training regarding what data is allowed to extract from an SPE. The verification can be done e.g. via: ○ a mandatory checkbox in a form SPE owners need to fill in for adding the role to extract data to the SPE user profile. ○ an e-mail from the SPE user organisation to the SPE provider, stating that the SPE user has received training.
P23	File extraction	**File extraction notification** It is recommended that the SPE provides a warning notice to the clarified SPE user (P22) prior to extracting files.	A warning notice to the clarified user prior to extracting data contributes to that files are not extracted by mistake.	Recommended	• When the clarified SPE user initiates a file extraction, a pop-up or additional page is displayed. This clearly states that the user is about to extract a file from the SPE and that only non-personal data is allowed to extract. The user needs to verify the initiated extraction before it is executed.
P24	File extraction	**Logs of file extraction** The SPE provider must keep tamper proof and identifiable logs of when files are extracted and by whom.	Logs of file extraction activities provide a basis for accountability for the SPE user in the process of controlling that only non-personal data is extracted.	Mandatory	• Logs of extraction of files from the SPE include: ○ User identity of the person that performed the extract. ○ Date and time for the extraction (clocks are synchronised with approved time sources).

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
					○ Filename, size and type of the file that was extracted. • Logs of extraction are sent to a dedicated log server at the SPE provider that have functionality to ensure that the integrity of the logs are preserved. • Logs of extraction are retained for one year. This has been decided on the following main considerations: ○ Most incidents where these logs may need to be used are discovered within this time. ○ The amount of logs generated for this period of time is reasonable considering available resources.
P25	File extraction	**Review of file extraction** The SPE must have functionality to allow the SPE user organisation to review the data in the files that have been extracted.	There are currently no technical controls that can verify that only non-personal data is extracted from the SPE. Functionality to allow for a manual review by a competent person will increase the possibility to detect extraction of personal data. The manner to implement this requirement is left quite open until further guidance is provided in relation to requirements in the EHDS regulation. Regardless, it is necessary that the extracted files (or a copy) are available until the review has been performed by the SPE user organisation.	Mandatory	• The SPE is set up to require review and approval by the SPE to ensure that the data in the files to be extracted only contains non-personal data. Either before each extract or on a sample basis based on risk. • A copy of extracted files is available to the SPE owner for review to ensure that files that have been extracted only contain non-personal data. Either for each extract or on a sample basis based on risk. • An AI has been trained to detect whether files to be extracted from the SPE only contain non-personal data. Manual review and approval

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
					by SPE owner are required when the AI flags a deviation.
P26	Storage	**Encryption of data at rest** All data in the SPE shall be encrypted at rest in line with current strong encryption standards.	Encryption of data at rest is a well-established good practice that is generally expected to be in place when handling sensitive data. There may be scenarios where this may cause performance issues and/or high cost when handling large amounts of data or if the processing activities require a high frequency of writing to and reading from the storage media. Such scenarios must however be handled as exceptions with specified and well-documented compensating controls to achieve a similar level of protection.	Mandatory	• All data in the SPE is encrypted when it is stored on hard drives.
P27	Storage	**Backup** The SPE provider shall provide backup services with backup frequency and retention time (minimum and maximum) to be determined by the SPE user organisation.	The need for backup will vary and will normally drive cost, and use of backup services must be determined by the SPE user organisation. However, it is important that the SPE provider can provide backup services within the SPE to avoid increased risk of extraction of other than non-personal data.	Mandatory	• The SPE provider includes weekly backup that is overwritten after 5 weeks in their SPE service. More frequent backup or longer retention time is available for additional cost. • The backup service of the SPE provider allows the SPE owner to decide which data in the SPE that shall be included in a defined backup plan. • The SPE provider offer offsite storage of backup.
P28	Storage	**Archiving** The SPE must allow for archiving services within the SPE infrastructure, or provide secure procedures to transfer data to external archive services.	It is important that the SPE provider can provide secure means for archiving to avoid increased risk of extraction of other than non-personal data.	Mandatory	• The SPE provider offers an archiving service that is designed for long-term storage within the SPE infrastructure. There are mechanisms to ensure that no one

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
					has access to change the data in the archive space. • The SPE provider offers a secure integration to a number of defined archive services.
P29	Analysis environment	**Analysis and data management capabilities** The SPE provider must have secure procedures for making analysis and data management capabilities and tools available based on user needs.	The need for tools within the SPE is expected to differ based on user needs and change over time. The main principle is that any tool may be allowed, but the associated risks need to be assessed and documented. It is imperative to minimise the risk of data leakage out of the SPE and that any incidents in the SPE will not affect other SPE instances.	Mandatory	• The SPE provider offers a set of analysis and data management capabilities per default. • The SPE provider has procedures to manage the need for additional capabilities. • Procedures and responsibilities for updates and licencing of both default and additional capabilities are clear. • Some tools require limited outbound calls to a defined licensing server to function within the SPE. Each such connection is assessed, documented, and monitored to ensure it cannot be used to circumvent file extraction controls.
P301	Analysis environment	**Separation of environments** Different SPEs at the SPE infrastructure must be technically separated.	It is important that there is a robust separation of different SPEs. This will prevent data leakage between SPEs and ensure that unwanted incidents in one SPE affects other SPEs. Separation of environments is a prerequisite to be able to allow more freedom for the activities performed in each SPE, such as importing own tools and code.		• The SPE infrastructure uses virtualisation technologies to ensure that different SPE instances are logically separated from each other. • Separation of SPEs within an SPE infrastructure together with transparent overview of roles and responsipilities is defined.

Nr	Area	Requirement (with title)	Comment / Guidance / Rationale	Importance	Examples of implementation
P31	Storage	**Termination of SPE** The SPE provider shall have defined procedures for termination of an SPE.	It is important that there exists a clear procedure for termination of the SPE.	Mandatory	• The SPE owner has a procedure that defines minimum actions when termination is to take place. These actions include deletion of files and folders, removing of users access rights, license software, back-up and logfiles etc.

Check list for SPE user organisations

This chapter contains a check list of requirements that are recommended to be in place at SPE user organisations. There are many regulations and standards that SPE user organisations need to comply with, and activities that are important when using an SPE. This check list focus on the activities that are necessary to directly complement the requirements in the SPE provider check list related to the requirements in the EHDS regulation[6]. The connection between the different check lists, in this document, is intended to provide a clear division of responsibility between the SPE user organisation and SPE provider. The check list for SPE user organisations can be a help for several different actors, including:

- SPE user organisations in assuming their data controller responsibilities when processing health data for secondary purposes.
- Health Data Access Bodies (such as Health Data Services) when providing guidance regarding use of SPEs.
- Audit authorities when assessing SPE user organisations for compliance with regulation related to processing of health data for secondary purposes.

[6] See mapping in (Attachment) Relation to EHDS, Article 73 – Secure Processing Environment

Below is a description of the different columns in the check list table.

- **Nr** – Enumeration of the requirements for easier reference. Starts with a U for User organisation.
- **Area** – Grouping of the requirements for easier reference.
- **Requirement** – Description of the requirement. Includes a title for easier reference.
- **Comment/Guidance/Rationale** – Description intended to explain the reason why the requirement is included in the check list and point out specific circumstances that may be relevant for the requirement. This includes relation to specific requirements in the SPE provider check list.
- **Importance** – All requirements are recommended to be mandatory at SPE user organisations when it comes to use of SPE services. It is recommended that any deviations are assessed and documented.
- **Examples of implementation** – Description of examples of different alternatives of how a requirement can be implemented, or different activities/functionality that may be relevant for implementation.

Nr	Area	Requirement	Comment / Guidance / Rationale	Importance	Examples of implementation
U1	ISMS	**ISMS scope** The scope of the ISMS at the SPE user organisation must cover the organisational units of the SPE owners and SPE users.	To have an ISMS in place is already a requirement from other laws (including GDPR). It is important to ensure that the ISMS at the SPE owner is valid for the activities related to the secondary use of health data within the organisation.	Mandatory	• Policy documents show that there is a clear connection between the overall ISMS of the SPE user organisation and the security requirements closely related to the secondary use of health data within the organisation.
U2	Access	**Manual identification** For SPE users that cannot log in using an eID with high level of assurance according to eIDAS, the SPE user organisation must verify the identity by having the SPE user identify with a passport or national ID card.	An important part of having control over the data in the SPE is to be able to verify that the persons that gain access are who they claim to be. Technical solutions for eIDAS level high are not yet fully available to cover for access to SPE users that are not residents in Norway. Therefore, there is need for a manual	Mandatory	• Verification of passport or national ID card is part of the standard background check in the onboarding routine for all type of personnel at the SPE user organisation. • The SPE owner requests that SPE users without BankID from external affiliates present their valid

			alternative routine to verify the identity of the user. Further focus on requirements related to personnel security is to be expected based on the suggestion for changes in existing Norwegian regulation to allow for background check for personnel in critical positions and functions that have access to large data sets with health data[7]. **SPE provider requirement "P4 – Identification level"** depends on that the SPE user organisation verifies the identity for users that cannot provide an eID with high level of assurance according to eIDAS.		passport or national ID card, prior to requesting access to the SPE for them. The procedure at the SPE user organisation requires that the SPE owner retain documentation of that validation of identification of affiliates has been performed.
U3	Access	**Verification of organisation affiliation** For any SPE users that are external to the SPE user organisation, it must be verified that the SPE user works at the organisation they claim to and that necessary agreements are in place.	This is one of several controls ensuring that the SPE user has a valid reason to have access to the data. Technical solutions do not yet have full support for this, but manual procedures may be used. This requirement can also be implemented at the **SPE provider** through the **requirement "P5 – Verification of organisation affiliation"** that is recommended for the SPE provider.	Mandatory	• The SPE user organisation has a standard procedure to request verification from external affiliates that new project participants are employed at the affiliated partner. • The SPE owner verifies that project participants from external affiliates use the official work e-mail from the affiliated partner when an SPE user account is created. • The SPE user organisation has selected an SPE infrastructure that provides a log on solution where the user eID has a property that link the user to their employer organisation

[7] Høring - krav om bakgrunnssjekk - regjeringen.no

					and this property is checked at log on to the SPE. (Functionality that may be possible to implement with eIDAS 2.0).
U4	Access	**Access approval** The SPE user organisation must have controls in place to ensure that only SPE users that are in the current data permit are approved access to the SPE by the SPE owner.	General access management procedures are expected to be in place as part of the ISMS. It is imperative that these procedures include limiting access to the SPE only to the people in the data permit. **SPE provider requirement "P7 – Access approval"** will help ensuring that the SPE has functionality for the SPE owner to add user access to the SPE and that only valid access requests are accepted. Implementation of SPE provider requirement "9 – Access according to data permit" would further help in automating this process.	Mandatory	• The general access management procedure at the SPE user organisation includes requirements for documented manager approval of new access rights. Access to an SPE is also defined as a high-risk role in the procedures for personnel security. • The routine for access management in a project SPE, specifies that only the SPE owner can approve access and that only persons in the related data permit can be granted access. • Access requests and approvals are documented and retained in the IT service desk system at the SPE user organisation prior to sending the access request to the SPE provider. • The SPE user organisation use the log of access requests at the SPE provider to document access approvals by the SPE owner and any defined delegates. The log of access requests is easily available to the SPE user organisation and the SPE provider is required to retain the log for at least two years.
U5	Access	**Removing access** The SPE user organisation must have controls in place to ensure that access is removed for SPE users that no longer shall have access to the SPE.	General access management procedures are expected to be in place as part of the ISMS. It is imperative that these procedures	Mandatory	• The general access management procedure at the SPE user organisation includes requirements for removal of access rights when they are no longer needed.

			include limiting access to the SPE only to the people in the data permit. **SPE provider requirement "P8 – Removing access"** will help ensuring that the SPE has functionality for the SPE owner to remove user access.		- The routine for access management in a project SPE, specifies that the SPE owner is responsible for ensuring that access rights are removed as soon as a user is no longer involved in the project.
U6	Access	**Review of access** The SPE user organisation must perform regular review of user access rights in the SPE to ensure that they are in line with the current data permit.	General access management procedures are expected to be in place as part of the ISMS. It is imperative that these procedures include limiting access to the SPE only to the people in the data permit. **SPE provider requirement "P10 – Review of access"** will help ensuring that the SPE has functionality for the SPE owner to perform regular review of access.	Mandatory	- The general access management procedure at the SPE user organisation includes requirements for regular review of access rights. - The routine for access management in a project SPE, specifies that the SPE owner must review access in the SPE quarterly. The results must be documented, and any deviations followed up. - The SPE owner obtain a list of all access rights in the SPE each quarter and verifies that only persons that should still have access and are listed in the permit have access. Documentation of the review is retained. - The SPE owner re-approves SPE user access every 6 months through an automatic function in the SPE user interface. The SPE provider is required to retain a log of access re-approvals for at least two years.
U7	Data import	**Register data import** Where the SPE infrastructure cannot receive data directly from data holders for import to the SPE, the SPE user organisation must have	Secure machine-to-machine transfer with strong end-to-end encryption from the data holder systems into the SPE is not yet	Mandatory	- The SPE user organisation has documented and communicated procedures for management of data from it is received from a data

		procedures in place to ensure that data obtained by the data holder is securely imported to the SPE and only used in the SPE.	available between all data holders and SPEs. It is therefore important that the SPE user organisation ensures that there are secure procedures to manage data from when it is obtained by the data holder until it is imported to the SPE. This requirement is especially important when the **SPE provider requirement “P17 – Machine to machine data transfer”** is not in place.		holder until it is imported into an SPE. This procedure includes restriction on what roles that can receive data, requirement of training for this role and prohibition from storing data anywhere else than in the SPE. • The SPE owner receives files from the data holder through a secure file transfer service. The SPE user use a secure interface to the SPE to import the data directly into the SPE. The data is removed from the area where it was received from the data holder. • The SPE user organisation regularly scan file storage spaces used by project members working with health data, with the objective of finding files that may contain directly or indirectly identifiable health data.
U8	File extraction	**Limit access to extract files** Access rights to extract data (unless it is certainly non-personal) must be limited to few individuals.	Limiting the number of users with access to extract files narrows down users to follow up. **SPE provider requirement “P21 – Role for extracting files”** will help ensuring that the SPE has a defined access role for extracting files which will make it easier for the SPE owner to control that only few individuals are granted this type of access.	Mandatory	• The SPE owner in a research project has assigned two project members the access role to be able to extract data. Data seldom needs to be extracted, so the task could probably have been covered by one person. The assessment is however that two people are necessary to provide robustness in the process. • In a large project there are several project members that continuously need to publish statistical data from different perspectives and often with short notice. Therefore the

					assessment has been to provide all these seven users with access to extract data from the SPE.
U9	File extraction	**User training on file extraction** All SPE users that shall have access rights to extract data from an SPE must obtain training regarding what data that is allowed to extract from an SPE.	Persons that have access to extract files from the SPE must to some extent be trusted to only extract files with non-personal data. Therefore it is important to ensure that such persons know what data that is allowed to extract. **SPE provider requirement "P22 – Verification of user training on file extraction"** depends on that the SPE user organisation can verify that the SPE user has received such training.	Mandatory	• The SPE user organisation has developed a standard training program for researchers that is mandatory for all employees and affiliated partners that will use an SPE. This training also focuses on that only non-personal data is allowed to extract from an SPE. The training goes into depth on what constitutes non-personal data and illustrates through examples what this means in practice for this specific research institution. • Prior to granting an SPE user an access role that can extract data, the SPE owner verifies that it is documented in the organisation's Learning Management System that the employee has performed mandatory training for use of an SPE.
U10	File extraction	**Review of file extraction** The SPE user organisation must have procedures in place to review that only non-personal data is extracted from the SPE.	There are currently no technical controls that can verify that only non-personal data is extracted from the SPE. Manual review by a competent person will increase the possibility to detect extraction of personal data. The manner to implement this requirement is left quite open until further guidance is provided in relation to EHDS requirements.	Mandatory	• The SPE is set up to require approval by a second authorised person prior to extraction of data. • Copies of extracted data is reviewed by the SPE owner. The above is done for all extractions or on sample basis based on risk. Documentation from the approval/review is retained.

			SPE provider requirement "P25 – Review of file extraction" will help ensuring that the SPE has functionality for the SPE owner to perform regular review of file extraction.		

(Attachment) Relation to EHDS, Article 73 – Secure Processing Environment

Below is an overview of how the requirements on Secure Processing Environments in the EHDS regulation is addressed through the recommended requirements in the check lists for SPE providers and SPE user organisations.

EHDS **Article 73** **Secure processing environment**	**Important minimum requirements**	**SPE provider**	**SPE user organisation**
1. Health data access bodies shall provide access to electronic health data ***pursuant to a data permit*** only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, ***the secure processing environment*** shall ***comply with*** the following security measures:	• An ISMS will cover technical and organisational measures for security on a general level. Ensuring a mature ISMS at both the SPE provider and SPE user organisation will be good preparation for more detailed requirements in Implementing Acts. • Requirements on machine-to-machine data transfer with end-to-end encryption from data holder to the SPE will decrease the use of manual steps in the data transfer process. If registers from NiPH (where the national HDAB is also located) transfer in this manner to the three SPEs at the major universities many use cases will be well prepared to comply with that the HDAB shall provide access only through an SPE. For use cases that cannot be covered by the	• ISMS P1-3 • Data import P16-17	• ISMS U1 • Data import U7

	requirements mentioned above it is pointed to the SPE user organisation responsibility when data is manually imported.		
(a) the restriction of access to the secure processing environment to authorised ***natural*** persons listed in the respective data permit;	- As long as the HDAB does not directly control access in the HDAB, it will be the access management procedures both at the SPE provider and SPE user organisation that will ensure compliance. - It is recommended that technical mechanisms are developed to ensure that only SPE users included in the current data permit have access to the SPE.	- Access P4-12 - Access P9	- Access U2-6
(b) the minimisation of the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art ***technical and organisational measures***;	- An ISMS will cover technical and organisational measures for security on a general level. Ensuring a mature ISMS at both the SPE provider and SPE user organisation will be good preparation for more detailed requirements in Implementing Acts.	- ISMS P1-3	- ISMS U1
(c) the limitation of the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;	- Robust access management procedures both at the SPE provider and SPE user organisation will be relevant to prepare for compliance with requirements in Implementing Acts.	- Access P4-12	- Access U2-6
(d) measures ensuring that ***health*** data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;	- Robust access management procedures both at the SPE provider and SPE user organisation will be relevant to prepare for compliance with requirements in Implementing Acts.	- Access P4-12	- Access U2-6
(e) the keeping of identifiable logs of access to ***and of activities in*** the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment; ***logs of access shall be kept for at least one year;***	- Functionality for logging of access to and relevant activities in the SPE will prepare for compliance with requirements in Implementing Acts.	- Logging P13-15	

(f) measures to ensure compliance with and the monitoring of the security measures referred to in this Article to mitigate potential security threats.	• ISO27001 certification at the SPE provider may be leveraged to some extent by external auditors that are to ensure compliance.	• ISMS P3	
2. Health data access bodies shall ensure that electronic health data ***from health data holders in the format determined by the data permit*** can be uploaded by those ***health*** data holders and can be accessed by the ***health*** data user in a secure processing environment. ***Health data access bodies shall review the data included in a download request to ensure that the health*** data users ***are*** only able to download non-personal electronic health data, ***including electronic health data in an anonymised statistical format,*** from the secure processing environment.	• Machine-to-machine data transfer with end-to-end encryption from data holder to the SPE will be good preparation to ensure compliance with the requirement that health data holders shall upload data into the SPE. • Mechanisms for restricted and controlled export of data and review of files that are exported from the SPEs will prepare for compliance with review to ensure that only non-personal data is downloaded. Potentially similar technical mechanisms at the SPE provider that are used by the SPE user organisation may be used if the HDAB is required to perform such review through Implementing Acts and future guidance.	• Data import P16-17 • File extraction P19-25	• - • File extraction U8-10
3. Health data access bodies shall ensure that audits of the secure processing environments are carried out on a regular basis***, including by third parties, and take corrective action for any shortcomings, risks or vulnerabilities identified by those audits in the secure processing environments***.	• ISO27001 certification at the SPE provider may be leveraged to some extent by external auditors that are to ensure compliance.	• ISMS P3	
4. ***Where recognised data altruism organisations under Chapter IV of Regulation (EU) 2022/868 process personal electronic health data using a secure processing environment, those environments shall also comply with the security measures set out in paragraph 1, points (a) to (f), of this Article.***	Data altruism is not specifically discussed in this report.		
5. ***By ... [two years from date of entry into force of this Regulation],*** the Commission shall, by means of implementing acts, lay down the technical,	Implementing Acts will be issued by the Commission.		

organisational, information security***, confidentiality, data protection*** and interoperability requirements for the secure processing environments***, including the technical characteristics and tools available to the health data user within the secure processing environment.*** Those implementing acts shall be adopted in accordance with the ***examination*** procedure referred to in Article 97(2).			