

# Travel Guide for PET implementation in Healthcare

## Authors

Sarah van Drumpt, Bastiaan van Schijndel, Joris Holtrop, Jannick Dorresteyn,  
Onno van der Galien, John de Vries, Steven Noorlander, Martine van de Gaar,  
Eric Boersma, Rogier Barendse, Isabella Kardys, Henk Marquering, John Jacobs

# Content

<b>Introduction</b>	<b>3</b>	<b>4. Checklist for the journey</b>	<b>12</b>
<b>1. The Departure Hall – Why take this journey?</b>	<b>5</b>	<b>5. Practical considerations: navigating uncharted territory</b>	<b>13</b>
<b>2. The Roadmap: Structure and tracks</b>	<b>6</b>	<b>6. Destination: safely shared insights</b>	<b>14</b>
2.1 Personas along the way	8	<b>7. Ready for Departure: Call-to-Action</b>	<b>15</b>
2.2 Stations	9		
2.3 Decision points at each stage	10		
<b>3. Travel documents &amp; instruments</b>	<b>11</b>		
3.1 Regulatory perspective	11		
3.2 Organizational perspective	11		
3.3 Collaboration perspective	11		

The background of the slide is a deep blue with abstract, glowing light blue and white wavy lines that sweep across the lower half. Scattered throughout are numerous circles of varying sizes and opacities, some appearing as solid blue or teal, while others are translucent or have a soft glow. The overall effect is a sense of dynamic energy and digital connectivity.

# Introduction

This guide is intended for healthcare professionals who (wish to) participate in data-driven collaborations across organizational boundaries, with a focus on making data available while safeguarding privacy. It provides a clear roadmap for the implementation of Privacy-Enhancing Technologies (PETs). Based on practical experience from the Secur-e-Health project, we describe organizational, legal, and technical steps, including personas and decision points. The emphasis is on situations where data enrichment is desirable or necessary but proves difficult to achieve due to technical limitations, privacy regulations (such as the GDPR), commercial interests, or a lack of mutual trust.

# Privacy-Driven Collaboration in Healthcare

## Objective

The Secur-e-Health project aims to enable secure, privacy-preserving analysis of health data across organizational boundaries. By leveraging advanced technologies such as multi-party computation and digital identity solutions, medical institutions can collaborate without directly sharing sensitive patient data. This supports the development of predictive models, more efficient treatments, and accelerates clinical research.

**Duration:** November 2021 – December 2025

**Program:** ITEA 4 (Eureka Cluster for Software Innovation)

**International Collaboration:** The project brings together 30 partners from five countries: Canada, Finland, Germany, Portugal, and the Netherlands.

- > **Canada:** Kelvin Zero, DENTOS Inc., Perceiv Research Inc.
- > **Finland:** Bittium, CSIT, MediConsult, Nordic Healthcare Group, Solita Oy, SUCCESS CLINIC, VTT
- > **Germany:** OFFIS, Oncare, Stryker, University Hospital Aachen
- > **Portugal:** Fundação Fernando Pessoa, ISP, MTG Research & Development Lab, University of Porto
- > **Netherlands:** Amsterdam UMC, Achmea, Almende, TU/e, Erasmus MC, Linksight, Medrecord, Ortec, PS-Tech, Stichting ZorgTTP, UMC Utrecht, TNO

## Use Cases:

The project includes several use cases, such as:

- > **Canada:** Development of a secure and user-centric digital identity solution to support the world's largest virtual clinical trial, integrating innovative authentication methods and patient involvement at every stage.
- > **Finland:** Use of federated learning to develop risk models for cardiac rehabilitation by combining data from multiple healthcare providers.
- > **Germany:** Implementation of a digitized patient pathway for treating femoral fractures, including computer-assisted surgery and sensor-based rehabilitation, using federated learning for data analysis.
- > **Portugal:** Deployment of federated learning to support smart pediatric care, focusing on clinical challenges such as addressing childhood obesity and post-surgical recovery, while ensuring patient data privacy across institutions.
- > **Netherlands:** Use of privacy-enhancing technologies to develop personalized risk scores for cardiovascular diseases based on electronic health records.

Secur-  
e-Health 



## ***Secur-e-Health:***

***"The future of data use in healthcare lies in investment and collaboration in the field of privacy."***

# **1. The Departure Hall – Why take this journey?**

Privacy-Enhancing Technologies (PETs) have become an indispensable part of modern data usage within healthcare. These technologies enable the (re)use of data for research, policy-making, and innovations such as measuring effectiveness of interventions, comparing healthcare institutions, and developing smart AI solutions. For policy purposes, data can be used to analyze trends in healthcare utilization and adjust national guidelines or funding models accordingly.

At the same time, PETs protect sensitive (health) data. These technologies support compliance with European privacy regulations (such as the GDPR), by minimizing the data usage and ensuring data is used for clearly defined purposes. PETs not only enable secure (re)use of data - as intended by the new European legislation, such as the European Health Data Space (EHDS) - but also enhance digital resilience by reducing the risk of data breaches.

For more information about the technologies themselves, we kindly refer to: [Information Commissioner's Office – Privacy-Enhancing Technologies](#).

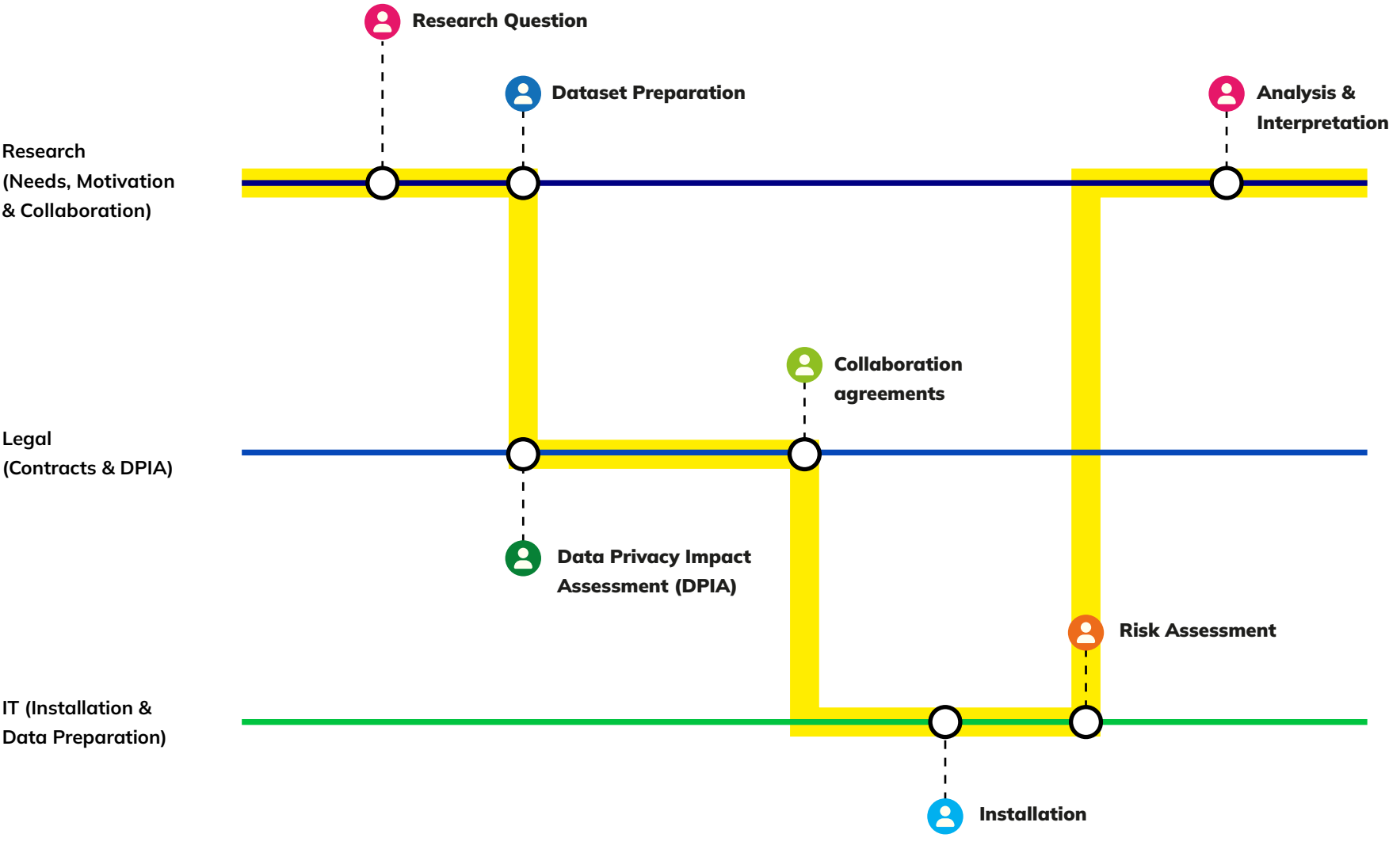


An abstract graphic featuring vibrant blue light trails that curve and converge towards the center, set against a dark blue background. Scattered throughout are semi-transparent blue circles of various sizes, creating a sense of depth and motion.

## 2. The Roadmap: Structure and tracks

The process of PET implementation can be compared to a journey along a carefully charted roadmap, where different tracks come together and intersect. Each track represents an important aspect of the implementation, from IT and technical preparation to legal requirements and research. The roadmap below offers an overview of the three main tracks that shape the journey through this process: IT (Installation & Data Preparation), Legal (Contracts & DPIA), and Research (Needs, Motivation & Collaboration). The roadmap shows a structured route, but in practice it is not a strict waterfall model: frequent back-and-forth communication occurs between stations to reach the right decisions and keep moving forward. We begin at the starting point, the ambition to collaborate, and travel through various stations toward the final destination: the structural embedding of privacy-friendly data sharing.

# Stations PET data collaboration



## What does the tour guide arrange?

- Researcher**  
Data management plan; variables, definitions, source agreements
- Data Manager**  
Dataset specifications; tools, format, and quality requirements
- Privacy Officer**  
DPIA, privacy principles
- Legal Counsel**  
Data processing or collaboration agreements
- IT/System Administrator**  
Technical requirements, installation planning, DMZ architecture (if applicable)
- Security Officer**  
Risk assessments, penetration tests (if applicable), benchmarking

Stage	Decision point	Key decision questions
Research Question	Preliminary Assessment	Are PETs appropriate (note: the answer also depends on the data availability)? What alternatives exist and what risks are involved?
Dataset Preparation	After Defining Data Requirements	Is the data available and in the correct format? Does it comply with legal and ethical criteria?
DPIA	After DPIA and Ethical Review	Should we proceed? Are the risks acceptable and legally covered?
Installation & Risk Assessment	After Technical Preparation	Is installation feasible? Does it meet security and infrastructure requirements?
Analysis & Interpretation	Before Execution	Are contracts, approvals, and security checks completed?

## 2.1 Personas along the way

Below are the various roles and responsibilities necessary for managing data and safeguarding privacy within an organization. It is important to emphasize that role titles may vary across organizations, and certain roles may be fulfilled by one or more individuals, depending on the organizational structure and the specific needs of the project. Defining roles and responsibilities not only ensures efficient execution of processes but also supports compliance with laws and regulations.

The following personas are relevant within this domain, each with their specific responsibilities:



### Researcher

As a researcher, I formulate the research question and determine the data requirements. I define variable specifications, make agreements about data sources, and carry out the analyses. Within a PET environment, I ensure that analytical integrity is maintained despite the limitations of the technology. This requires careful preparation, clear coordination, and robust validation methods to ensure the reliability of the results. Ideally, I apply the [FAIR-principles](#) (Findable, Accessible, Interoperable, Reusable) to enhance the value and reusability of data and analyses. I translate the outcomes into clear insights that contribute to better decision-making or improvements in care.



### Data Steward

As a data steward, I am responsible for the extraction, transformation, and harmonization of data. I ensure that datasets are of high quality, stored according to standard data formats, and carefully curated, so they remain consistent, usable, and future-proof. I also maintain communication with researchers and other data partners to ensure that data is shared consistently and well-coordinated, allowing the research process to run smoothly.



### Privacy Officer

As a privacy officer, I support the execution of Data Protection Impact Assessments (DPIAs) and monitor privacy principles within the project. I advise on measures the researcher can take to mitigate privacy risks. If our organization has appointed a Data Protection Officer, we consult them for advice during a DPIA. Together with the researcher, I complete the privacy matrix and evaluate the traceability of data. I also work closely with legal and IT teams to ensure compliance with privacy legislation and to safeguard the protection of personal data.



### Legal Advisor

As a legal advisor, I draft data processing agreements and data transfer agreements, and ensure that formal roles and risk characteristics are correctly documented in contracts. I provide guidance on legal frameworks such as the GDPR and the European Health Data Space (EHDS), and ensure that the project complies with applicable laws and regulations, minimizing legal risks related to compliance.



### IT/System administrator

As an IT or system administrator, I am responsible for the technical setup and maintenance of the PET environment within our infrastructure. I handle the installation, configuration, and monitoring of the systems. In doing so, I ensure the availability and reliability of the infrastructure and make sure it aligns with existing architectures (such as DMZ and network segmentation). Collaboration with security and privacy colleagues is essential to ensure that the PET software not only works, but is also secure and scalable.



### Security Officer








As a security officer, I assess the security risks associated with the use of PETs. I conduct risk analyses, evaluate threats, and commission penetration tests where necessary. My role is to ensure that the chosen technical and organizational measures match the sensitivity of the data and the use case. I advise on additional measures and continuously monitor the security posture so that cross-organizational collaboration meets high standards of information security.



## 2.2 Stations

Experience shows that the process of PET implementation consists of several stations, with a different guide taking the lead at each phase. The guide ensures that the necessary actions are taken to confidently pass the station and continue the journey.

The table below outlines the stations, the guide, the guide's objective, and an insight to help them consciously address the specific challenges of each phase.

Station	Guide	Track	Objective	Note
Research Question	 Researcher	Research	Define a clear data need and enable PET analysis without identifiable data	Knowledge of available data sources and their structure is essential
Dataset Preparation	 Data Manager	Research	Extract, harmonize, and prepare data in the correct formats	Errors in data are hard to detect at a later stage
DPIA	 Privacy Officer	Legal	Identify and mitigate privacy risks through DPIAs and privacy principles	PETs reduce risk but does not replace legal due diligence
Collaboration Agreements	 Legal Counsel	Legal	Contractually define responsibilities and risks	Technology alone is not enough; formal agreements prevent misunderstandings
Installation	 IT/System Administrator	IT	Securely integrate PET software into the infrastructure	Custom installation requires cross-departmental collaboration
Risk Assessment	 Security Officer	IT	Assess security risks within specific use cases	Risks vary per use case; reassessment is needed for each case
Analysis & Interpretation	 Researcher	Research	Perform analysis within PET constraints, interpret and validate results	Subtle errors can easily go unnoticed; extra validation and interpretation are essential

## 2.3 Decision points at each stage

At each stage, we recommend to stop and consider whether the implementation of the PET is still contextually appropriate, taking into account factors such as data availability, legal and ethical considerations, technical feasibility, and security requirements. The table below provides an overview of these decision points and the key questions that must be answered to successfully proceed through the process.

Stage	Decision point	Key decision questions
Research Question	Preliminary Assessment	Are PETs appropriate? What alternatives exist and what risks are involved?
Dataset Preparation	After Defining Data Requirements	Is the data available and in the correct format? Does it comply with legal and ethical criteria?
DPIA	After DPIA and Ethical Review	Should we proceed? Are the risks acceptable and legally covered?
Installation & Risk Assessment	After Technical Preparation	Is installation feasible? Does it meet security and infrastructure requirements?
Analysis & Interpretation	Before Execution	Are contracts, approvals, and security checks completed?

# 3. Travel documents & instruments

During the implementation of PETs, several documents and instruments are relevant from three perspectives: regulatory, organizational, and collaboration. These documents help ensure compliance with laws and regulations, organize processes efficiently, and facilitate cooperation among various stakeholders. This chapter discusses the key documents and instruments needed to successfully navigate the PET implementation journey.

## 3.1 Regulatory perspective

From the regulatory perspective, legal and policy requirements are central in framing the use of PETs. These documents ensure compliance with privacy legislation and provide guidance for defining responsibilities. They form the basis for lawful and transparent data processing.

- > **DPIA:** mandatory risk assessment for projects with potentially high privacy risks.
- > **(Joint) Data Processing Agreement:** formalizes roles and responsibilities regarding data processing. This includes specifying which data will be processed and under what conditions.

## 3.2 Organizational perspective

From an organizational standpoint, several elements contribute to a structured and secure PET implementation. These relate to process design, availability of expertise, and technical prerequisites. The following documents and measures support robust execution and governance within the organization:

- > **Risk Assessment:** evaluation of threats, vulnerabilities, and impact.
- > **IT Architecture & Documentation:** DMZ, network segmentation, access protocols.
- > **Data Management Plan:** roles, definitions, classifications, data flows, and FAIR principles.
- > **Capacity & Expertise:** availability of data, privacy, security, and technical specialists.

## 3.3 Collaboration perspective







Effective collaboration between involved parties is crucial for PET deployment. This perspective focuses on agreements, coordination, and shared working methods necessary to ensure a common understanding and smooth cooperation. The following instruments support transparent and aligned collaboration:

- > **Joint Privacy Matrix:** agreements on identifiability and data usage, jointly evaluated against privacy principles and measures relevant to the data collaboration.
- > **Data Transfer Agreement:** for the exchange of sensitive data.
- > **IT coordination:** infrastructure, monitoring, and maintenance via architecture diagrams.
- > **Researcher meetings:** joint discussion of final results.

## 4. Checklist for the journey

For successful PET implementation, certain tasks must be managed along the way. This checklist, organized per persona, outlines the key responsibilities and actions for each role in the process. By taking the right steps at the right time, privacy, security, and other essential aspects can be efficiently managed.

### Checklist per persona

Role	Responsibilities / Actions
 Researcher	Data management plan; variables, definitions, source agreements
 Data Manager	Dataset specifications; tools, format, and quality requirements
 Privacy Officer	DPIA, privacy principles
 Legal Counsel	Data processing or collaboration agreements
 IT/System Administrator	Technical requirements, installation planning, DMZ architecture (if applicable)
 Security Officer	Risk assessments, penetration tests (if applicable), benchmarking

**Tip:** Collect all technical and content-related details in advance to allow efficient privacy and security review.

# 5. Practical considerations: navigating uncharted territory

Since PETs are relatively new, implementation often takes place in unfamiliar territory. This requires extra awareness of various aspects to safely and successfully complete the journey. Key considerations and practical guidance include:

## **Legal and administrative embedding:**

PETs often require a dedicated section in existing DPIAs and contract templates.

**Helpful approach:** use standardized formats, such as adapted DPIA templates, and examples from previous implementations (e.g., federated learning at UMC Utrecht).

## **Invisibility of data quality requires early assurance**

Raw data is not shared between parties, making input errors difficult to detect.

**Helpful approach:** involve domain experts early to ensure data selection and interpretation are accurate. Pilot analyses or simulations can also detect anomalies.

## **Higher security requirements in cross-organizational collaboration**

Collaboration between healthcare institutions and external parties requires robust technical and organizational security measures. Privacy-enhancing technologies contribute to this, but they are not a complete solution; additional measures remain necessary to cover all risks.

**Helpful approach:** reuse existing security assessments and audits where possible and follow proven technical standards.

## **Lack of familiarity and experience with PETs:**

Many organizations are unfamiliar with PET workflows and implications, which can cause delays or misunderstandings.

**Helpful approach:** provide practical examples, accessible explanations, and support (e.g., via open-source [PET-lab](#) or PET providers).

## 6. Destination: safely shared insights

The added value of PETs is discussed below, illustrated with a practical example from the Secur-e-Health project.

### Benefits of PETs:

- > **Improved models through combined data:** integrating data from multiple sources leads to more robust and accurate AI models.
- > **Population-specific fine-tuning and continuous updates:** models are continuously adapted to the unique characteristics and needs of specific patient populations.
- > **Guaranteed privacy protection:** advanced techniques such as federated learning and multi-party computation ensure patient data confidentiality.
- > **Enhanced trust in data-driven healthcare innovation:** transparency, security, and effectiveness increase acceptance of AI in healthcare.

### Practical example: Better cardiovascular risk prediction while preserving privacy

To better treat cardiovascular patients, it is crucial to predict their risk of disease progression or new conditions accurately. Two case studies illustrate how PETs improve data-driven models without compromising privacy or data control.

#### Case 1: Customized risk model for vascular patients

UMC Utrecht aimed to adapt the existing SMART2 model - which predicts the likelihood of a patient with existing vascular disease developing another condition - to their patient population. This required additional data from outside the hospital, such as information from insurer Zilveren Kruis. Data sharing between hospitals and insurers is sensitive and strictly regulated, requiring an adequate security level. A penetration test was performed to assess security measures, which informed risk management and technical configuration.

Using **secure multi-party computation**, data from both parties were combined securely without sharing underlying patient data. Each party retained control over its own data. This enabled:

- > Customizing the risk model for UMC Utrecht patients.
- > Retaining data control for both hospital and insurer.
- > Semi-automatic enforcement of data usage agreements through technical structures.

**Result:** an improved model aligned with patients, while maintaining privacy and trust.

#### Case 2: Improved heart failure prognosis with federated learning

Heart failure requires precise risk stratification. In collaboration among multiple university medical centers, routine lab data from electronic health records were analyzed using time-dependent Cox models to predict disease progression.

Due to distributed data, **federated learning** was employed: a PET technique allowing models to be trained on local data while maintaining privacy.

**Result:** PETs contributed to better predictive models for cardiovascular disease without compromising privacy, trust, or compliance.





## 7. Ready for Departure: Call-to-Action

To deploy PETs effectively in your data ecosystem, start with small, practical steps. This helps understand the added value of PETs in your specific context.

Recommended actions:

- > **Evaluate your data collaborations:** where does PET add value?
- > **Start a pilot analysis:** use templates and guidance from the Secur-e-Health project.
- > **Contact** the Secur-e-Health team for templates, demos, and advice. Andries Stam (CEO Almende b.v.); [Andries@almende.org](mailto:Andries@almende.org);

## Authors

- > Sarah van Drumpt, TNO (primary author), sarah.vandrumpt@tno.nl
- > Bastiaan van Schijndel, Stichting ZorgTTP (primary author), bastiaan.van.schijndel@zorgttp.nl
- > Joris Holtrop, UMCU, j.holtrop-3@umcutrecht.nl
- > Jannick Dorresteyn, UMCU, j.a.n.dorresteyn-2@umcutrecht.nl
- > Onno van der Galien, Zilveren Kruis, onno.van.der.galien@zilverenkruis.nl
- > John de Vries, Zilveren Kruis, john.de.vries2@zilverenkruis.nl
- > Steven Noorlander, Zilveren Kruis, steven.noorlander@zilverenkruis.nl
- > Martine van de Gaar, Linksight, martine@linksight.nl
- > Eric Boersma, Erasmus MC, h.boersma@erasmusmc.nl
- > Rogier Barendse, Erasmus MC, r.barendse@erasmusmc.nl
- > Isabella Kardys, Erasmus MC, i.kardys@erasmusmc.nl
- > Henk Marquering, Amsterdam UMC, h.a.marquering@amsterdamumc.nl
- > John Jacobs, Ortec, john.jacobs@ortec.com

