Bio-curity

D4.1 Security and Assurance Criteria for Qualified Data Framework

DELIVERABLE VERSION	V1.0
WORK PACKAGE	WP4 Data sovereignty, trust and security
TYPE	Document
CONTRACTUAL DATE OF DELIVERABLE	31/08/2023
ACTUAL DATE OF DELIVERABLE	08/09/2023
RESPONSIBLE PARTNER	TNO (TNO 2024 P11374)
DISSEMINATION LEVEL	Public
STATUS	Final

eureka

ecs

Table of content

Partners involved

Company	Name and surname	Email address
TNO	**Sarah van Drumpt / Dayana Spagnuelo / Kevin Witlox**	**sarah.vandrumpt@tno.nl dayana.spagnuelo@tno.nl kevin.witlox@tno.nl**
Lostar	**Murat Lostar**	**murat.lostar@lostar.com.tr**
KnowL	**Joanna Morozowska**	**joanna@medrecord.io**
	Jan-Marc Verlinden	**Jan-marc@medrecord.io**
Medron	**Cemre Arslan**	**cemre.arslan@medrontech.com**
Vestel Electronic	**Ilhan kaya**	**ilhan.kaya@vestel.com.tr**
Vestel Home Appliance	**Çağlar Ebeperi**	**Ismail.ebeperi@vestel.com.tr**
Kafein	**Serhat Taşkale**	**serhat.taskale@kafein.com.tr**

Changes tracker

This document is an amended version of the original Deliverable 4.1. In the table below we summarise the changes.

Affected area	Changes	Version
Overall document	Correction of typos and minor changes in text for increased readability. Improvement of references and images descriptions.	1.0
Section 3.2	More explanation is added about Self-Sovereign Identity technologies and the design choices that serve as input for the technological architecture.	1.0
Section 4.1	Clarification about the perspective taken for the risk evaluation.	1.0
Section 4.2.5	Change in title from "Healthcare and Ethics" to "Healthcare and Health Ethics".	1.0
Section 4.2.7	Further clarification about the impact of themes "retention" and "age restriction" in the selected criteria.	1.0

1. Introduction

In an ever-evolving landscape of technological advancements, the Bio-curity project embarks on a crucial mission to revolutionize the way we ensure security, trust, and privacy in the context of monitoring patients' personal and medical data derived from digital biomarkers within the home environment. The primary objective of T4.1 *Security and assurance criteria* is to determine relevant

criteria and components for the intended trust model that will meet stringent security and privacy standards and is fit for its purpose.

This deliverable marks a significant milestone in the Bio-curity project, as it outlines a comprehensive list of criteria and components necessary to realize the intended trust model. By transitioning the monitoring process to the home environment, we face unique challenges that demand innovative solutions. The security, integration, trust, and privacy requirements in this novel context create distinct constraints that require careful consideration and expert design. Our collective efforts aim to establish an firm foundation, ensuring the highest level of assurance for the generated data and safeguarding it both in transit and at rest. By creating a model that accurately represents the complexities of the home environment, we strive to harness the vast potential of medical data while instilling confidence in its security.

The successful realization of the qualified data framework will significantly impact the second task and its related deliverable D4.2 *Trust model technology architecture*. As we move forward over the course of the second task, the architectural framework will emerge, complemented by visualizations that vividly depict how our trust model seamlessly intertwines with the home environment and its existing infrastructure.

In conclusion, the document including the Security and Assurance Criteria for Qualified Data Framework is not just a technical document; it is a testament to our collective resolve to build a better, safer, and more reliable future for medical data monitoring within the comforting confines of our homes. Together, we strive to refine healthcare paradigms and elevate the standards of trust and assurance in the digital age.

1.1 Purpose of the document

This document provides a comprehensive list of themes and/or criteria to consider in the design phase, for those that intend to design a digital health technology that includes data exchange activities between parties in the health sector.

1.2 Context

As we move towards the era of personalized healthcare, the home environment takes centre stage as the nucleus of data generation and patient-centric monitoring. Qualified Data Exchange (QDX) is a model developed by TNO (Joosten, 2023). It suggests a way to design systems for the exchange of data between different organizations, taking as starting point the autonomy (sovereignty) of involved parties. QDX identifies roles involved in exchange of data from different perspectives (Figure 1 illustrates an overview of the model), and the conditions (criteria) under which data can be considered “qualified”, i.e., compliant to requirements and expectations of the involved parties. We take the QDX model as guide to come to criteria that are relevant for our Bio-curity platform. The QDX model proposes a bottom-up way of thinking about data exchange. This is not only about data syntax and semantics, but also about other characteristics of data that make them suitable or unsuitable for use

in given transactions between two individual healthcare institutions and/or professionals. QDX is also about governance and management processes in which supply and demand are formulated.

The QDX model is characterized by three primary layers, as depicted in the visual representation below. The top layer presents entities capable of providing data (referred to as QDX Management) and those requesting data (referred to as QDX Governance). The objective is to match the data supply and demand within a marketplace environment. Transitioning to the second layer, the policy layer, refers to policies that help to keep track of agreements, in laying down rules, provide guidance and preform audits. This layer can include policies related to data provisioning, requesting, and the selection of suitable infrastructure. The third and lowest layer includes the operational activities, containing the tangible data transfer processes facilitated by predetermined communication tools. These operations should align with the goals set in the highest layer.

Consequently, this report initiates its investigation into criteria by reaching out to the data-exchanging parties as represented in the uppermost layer. The aim is to comprehend their objectives and assurance prerequisites, which will fundamentally define the trajectory of our research. Through these discussions, we seek to ensure that the subsequent operations align with the intended purpose of the involved parties.

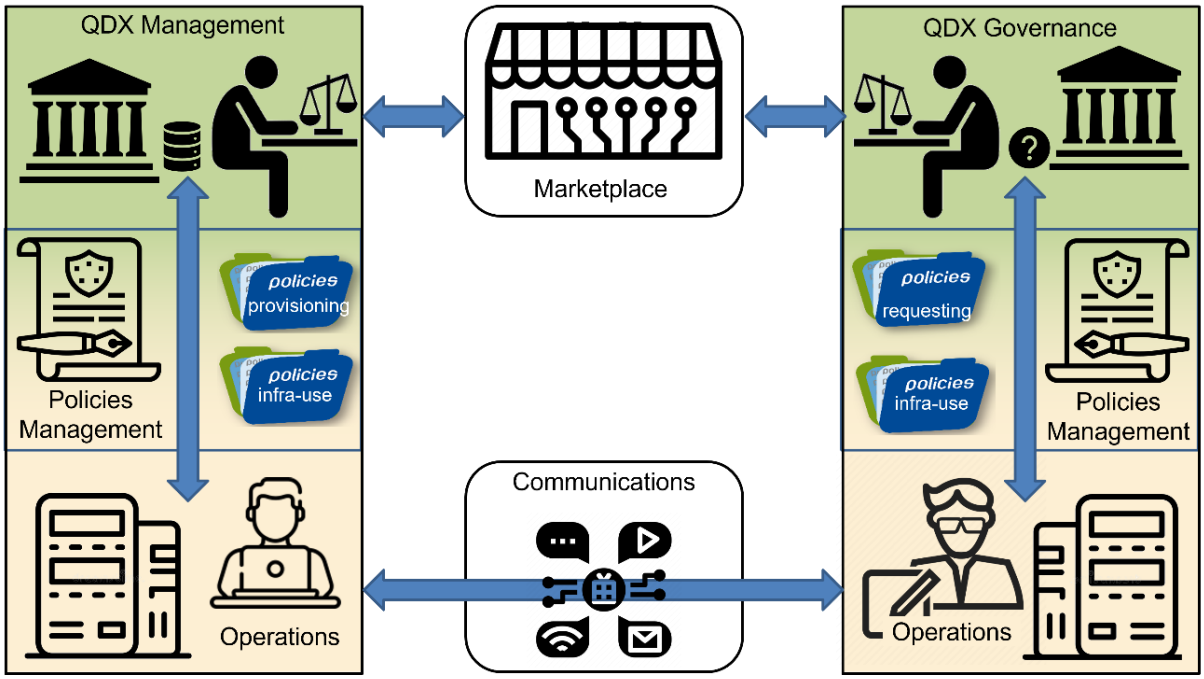

Figure 1 - Overview of Qualified Data Exchange model

1.3 Definitions

Acronym, Abbreviation	Meaning
TRL	Technology Readiness Level
GDPR	General Data Protection Regulation

QDX	Qualified Data Exchange
EHDS	European Health Data Space
ISO (/IEC)	International Organization for Standardization (/International Electrotechnical Commission)
NEN	Stichting Koninklijk Nederlands Normalisatie Instituut
AI	Artificial Intelligence
PPG	Photoplethysmogram
BLE	Bluetooth Low Energy
IoT	Internet of Things
ECG	Electrocardiogram
IMU	Inertial Measurement Unit
EHR	Electronic Health Record
OWASP	Open Worldwide Application Security Project

2. Methodology

The methodology used in this project is composed of two main phasis: 1) in order to understand the current data flow and propose a suitable approach for the future Bio-curity platform we use a **bottom-up** approach, this allows for topics to emerge naturally from consortium partners' ideas without much guidance or interference; and 2) for the elicitation of criteria we opt for a **top-down** approach, which helps consortium partners to ideate about needs and desires for future exchange of data.

Bottom-up. The data flow is conceptualised with the help of consortium partners. This project involves partners from both industry and academia, providing diverse health-related products with a wide range of Technology Readiness Levels (TRL). To initiate discussions, we distributed questionnaires to clarify their roles in the project, understand their goals, and unify the terminology used to describe these products. The questionnaire used explorative questions such as, "what is your role in the Bio-curity use cases?", "Where are you active in the data flow chain: data generation, transmission, storage, calculation/analysis, and visualisation?", and "which data do you use and for what desired health outcome? And what kind of data is it: continuous/discrete, structure/unstructured, micro/meta-data?".

Following the questionnaire, two focus groups were organized with domain experts delegated by consortium partners. In the first focus group we discussed the representations of current data flows, which emerged from the questionnaires. With the group discussion the flows were refined, and the interests of partners towards exchange of data emerged. The second focus group discussed the propositions for the future data flow which will be implemented in the Bio-curity platform. Three alternatives were discussed, and the partners feedback and concerns were collected from the discussion.

The Dutch and Turkish partners conducted this bottom-up approach in parallel, holding separate group discussions for each. The concluding step both were compared and merged. The results of this step are presented in Section 3 and are collected from the minutes of the focus groups, and related literature identified by the partners.

Top-down. The elicitation of criteria, on the other hand, was conducted in a top-down approach. The choice of approach was reactive to the fact that the project is in too early of a stage, and therefore partners are still maturing their ideas on how to best leverage the proposed exchange of data. This is one of the findings that emerges from the focus groups in the previous stage. In fact, when directly asked about what they considered crucial for a successful and secure data exchange (this is the essence the criteria try to capture), only preliminary ideas emerged about compliance with data protection regulations, and the need for quality assurance for the underlying data. Therefore, we search for criteria in relevant regulations and technical standards instead.

Regulation and standards on healthcare, and processing of data for health, is the corpus used for analysis in this second stage of the research. The selection of corpus was done via input from domain experts, particularly from the Dutch side of the consortium, as Turkish regulations are considered out of scope (Turkish regulations are for most part in line with current or previous European regulations, and in general less stringent, therefore compliance with European regulations is regarded as sufficient for Turkey as well). Regulations still in proposal phase are considered in scope, to ensure the Bio-curity platform is aligned with regulatory demands likely to apply in the near future. The selected corpus is listed below:

- Processing of personal and health data:
  - General Data Protection Regulation (GDPR)[i] – European regulation on data protection
  - Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg[ii] – Dutch regulation on the processing of personal data on health
  - Data Act[iii] – Proposal for European regulation on harmonised rules on fair access to and use of data
  - European Health Data Space[iv] – Proposal for European regulation on European Health Data Space
  - Wet elektronische gegevensuitwisseling zorg[v] – Proposal for Dutch regulation on electronic health data exchange
  - NEN 7513:2018 Health informatics (NEN, 2018) – Recording actions on electronic patient health records
  - NEN-EN-ISO/IEC 27701:2021 Security techniques (NEN, 2021) – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- Healthcare and health-related systems:
  - Wijzigingswet Burgerlijk Wetboek (geneeskundige behandelingsovereenkomst[vi]) – Dutch regulation for medical treatments
  - Wijzigingswet Wet cliëntenrechten zorg, enz. (taken en bevoegdheden op het gebied van de kwaliteit van de zorg)[vii] – Dutch regulation on health care client right
  - Regulation on medical devices[viii] – European regulation on medical devices

  - NEN 7510-1:2017 Health informatics (NEN, 2017) – Information security management in healthcare - Part 1: Management system
  - NEN 7510-2:2017 Health informatics (NEN, 2017)– Information security management in healthcare - Part 2: Controls
  - NEN 7512:2022 Health informatics (NEN, 2022) – Information security in healthcare - Requirements for trusted exchange of health information
- Automated processing of data:
  - Artificial Intelligence Act (AI Act)[ix] – Proposal for European Regulation on Artificial Intelligence

We test the relevance and completeness of our corpus by comparing it with the legal framework presented by MedMij (MedMij, 2023), the Dutch standard for secure exchange of health data between healthcare providers and patients. MedMij is selected for this test as one consortium partner (KnowL solutions) provides a MedMij certified PGO[1], and therefore their legal framework is of relevance for the project. Our corpus is more comprehensive and encompasses all, but the consumer laws presented in MedMij's framework, that is because of the relationship between care providers and users, which is not the main focus of our Bio-curity platform.

In order to extract criteria from our corpus we conduct a thematic analysis, which is a methodology for analysis of qualitative data with the goal of generating knowledge in a more systematic way yet based on subjective domain expertise (Nowell, 2017). We start by reading our corpus and selecting only the most relevant articles that refer to data, or rights and obligations with respect to the exchange of data. We import them in the supporting tool ATLAS.ti[2], and continue our analysis departing from the tool's automatically detected themes.

Two researchers work on refining the themes, starting from merging synonyms, then merging and grouping related themes, to finally filtering and removing codes unrelated to data exchange (technology or standards applicable to consortium partners individually, but not related to the Bio-curity platform, such as, management of joint-controllership) or broad non-informative (such as, "law"). The themes are categorised as relevant to one of the components in the platform: data, patients/subjects, providers (and their secure exchange of data), and the whole platform itself. This process results in 67 criteria, categorised in four main applicable categories, and two complementary categories which are deemed out of scope. These results are presented in Section 4.

3. Digital Health Solutions

In section 3.1 we first give an overview of roles and data flows of partners individually, prior to the envisioned Bio-curity platform. The data flow and applicable roles change depending on the stage of development of a product, and not each partner is involved in every development stage. As such, the solutions presented in section 3.1 have different levels of maturity, with some being already in place, while others depict upcoming developments. In addition, in section 3.2, we describe options for possible data flows in the Bio-curity platform that address trust and control issues.

[1] MedSafe

[2] ATLAS.ti | Software for Qualitative Data Analysis - ATLAS.ti (atlasti.com)

3.1 Roles and Data Flows – before Bio-curity

In the current digital health solutions of the Bio-curity partners, we distinguish five main roles when explaining the operationalisation process.

1. **Sensor Manufacturers** design, produce, and maintain the physical sensors that collect data from the environment or individuals. They ensure the sensors are accurate, reliable, and adhere to relevant standards. To enable this, they store data from the sensor. Some manufacturers interpret the data in question to show to the healthcare provider.
2. **Platform Manufacturers** develop the software or system that collects, processes, and manages data from various sources. This may include data from healthcare institutes, various sensors, laboratory values and medication. They provide the infrastructure for data storage, analysis, and visualization. Platform Providers may target either patients or healthcare professionals as their end-user, or both.
3. **Patients/Data subjects** are the sources of the data. They provide personal health-related information through wearable sensors or other means. They have control over their data and may need to grant permissions for its use.
4. **Health Practitioners** use the collected data to monitor, diagnose, and provide treatment to patients. They leverage the platform to access patient data and collaborate with other stakeholders.
5. **Researchers** analyse both individual data that can be traced back to a person, and aggregated and anonymized data that does not contain identifiers directly linking to a person, to derive insights, identify trends, and contribute to scientific knowledge. They use the data to conduct studies and make advancements in their field. They generally look for cohorts of data of larger numbers of patients to enrich their insights.

Note that an organisation is not limited to one role. For example, most organisations develop both sensors and conduct research on the data their sensors generate. In Figure 2 below we describe the focus areas of our Bio-curity partner in regards to data acquisition, data processing and model training, validation and testing.

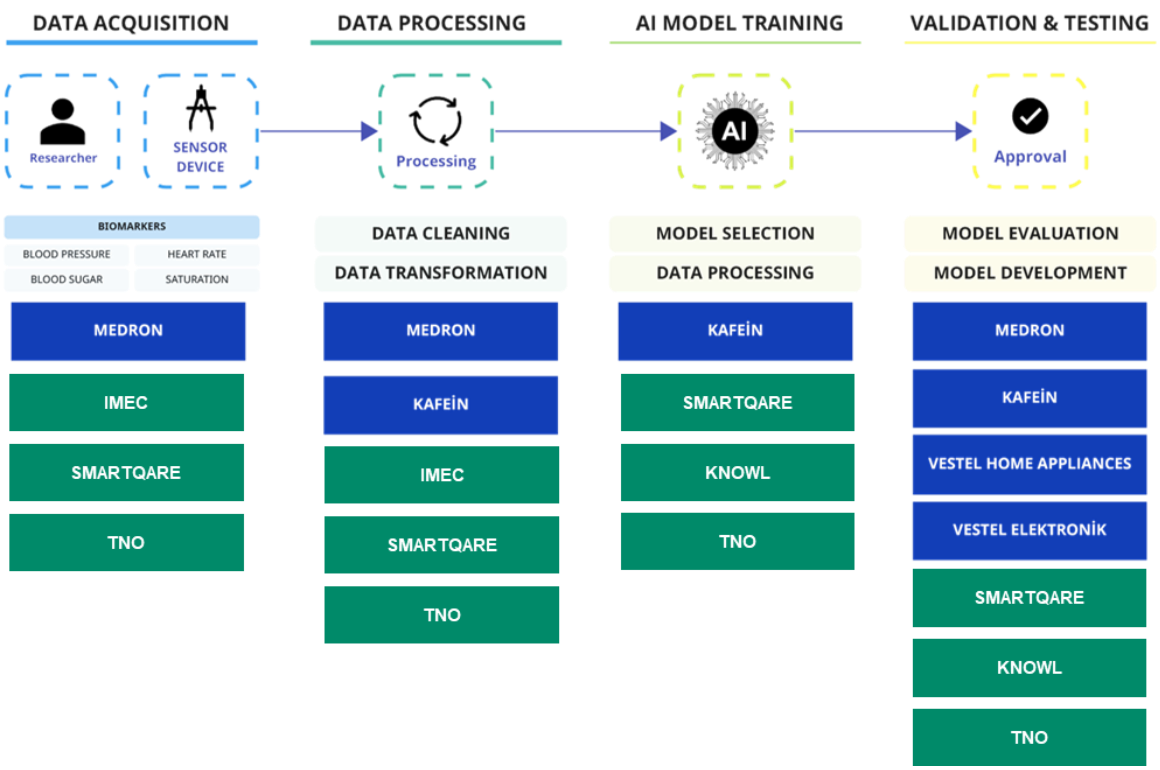

Figure 2 - Focus area of Bio-curity partners (Turkish partners in blue, Dutch partners in green)

Generally, data is generated in different phases of the development cycle of a digital health solution (Roche Information Solutions in collaboration with Prova Health, 2023). Each phase has its own purposes. For example, in the product development phase, data is often generated for qualitative studies. Whilst in the regulatory approval phase, data is often generated for risk assessment purposes. Depending on the phase, data is typically collected by a specific type organisation, accessed by certain people, encrypted or not, etc. Therefore, we describe the data flows of current digital health solutions according to the phase they are used in. We present one data flow per phase and country to illustrate what a typical data flow looks like among our Bio-curity partners in that specific phase, but note that partners are often active in multiple phases of the development cycle.

3.1.1 Post-market surveillance (A)

Post-market surveillance is the phase where observational studies using real-world data fit. Below you find a description of data flows pertinent to this phase (phase A in the development cycle),

taking a sensor device of one of our Bio-curity partners to illustrate (see Figure 3).

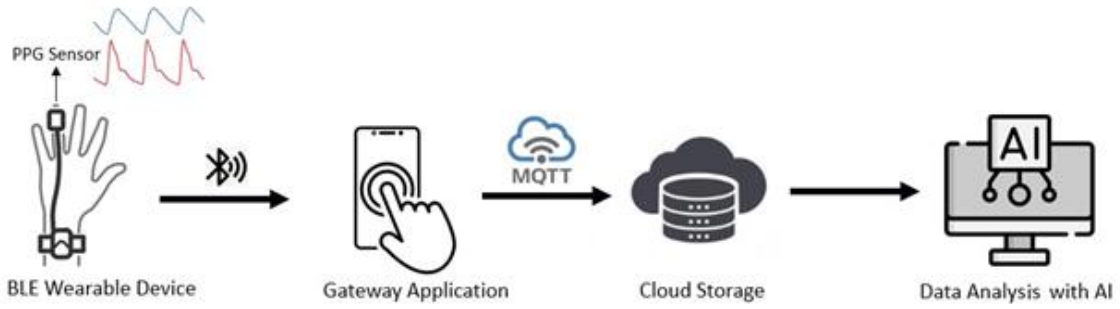

Figure 3 - Data flow for sensor device as an example pertinent to Post-market surveillance

- Purpose: Data is generated for observational studies. The aim is to detect atrial fibrillation using artificial intelligence methods based on pulse rate data obtained from finger PPG signals, body temperature, and raw PPG data.
- Sources: As a data source, a PPG sensor using infrared and red light, along with a 9-axis Accelerometer sensor, have been utilized.
- Activities: The project's activities encompass the utilization of various technologies. Bluetooth Low Energy (BLE) was employed for data transmission, BLE beacon broadcasting was utilized for location tracking, an IoT Gateway facilitated the transfer of data to the server, and artificial intelligence was applied for the analysis of the collected data.
- Roles: Sensor Manufacturers (please find the definition of this role at the beginning of this section)
- Data accessibility: The data has been employed within the scope of the described technology and is therefore only accessible by the project members of the manufacturers; the access of artificial intelligence to raw PPG data is structured through the project's database.

3.1.2 Product development (B)

Product development refers to the phase where qualitative and simulation studies are conducted, with some initial clinical validation of solutions and early user feedback. Below you find a description of two data flows pertinent to this phase (phase B in the development cycle), with the second taking a sensor device of one of our Bio-curity partners to illustrate (see Figure 4).

First data flow for usability testing in the product development phase

- Purpose: It aims to develop an experimental medical product with features that individuals can use without significantly affecting their daily lives. Basically, it is aimed to collect essential vital data such as heart rate and activity level. The purpose of gathering this data is to enable individuals to closely monitor their health and detect potential health issues at an early stage. The technical phases of the project commence with preliminary validation studies conducted using a reference device. In this phase, simultaneous test measurements are carried out using an ECG-based chest strap and a wearable PPG sensor. During these tests, a real-time interface is developed to visualize and monitor PPG data live. The pre-validation process involves

examining heart rate data obtained during exercise and observing the compatibility between data from the ECG-based reference device and the wearable PPG sensor. The data collected through the sensors used in the project will be stored and will be analysed later for health monitoring. This approach aims to enhance the effectiveness and user-friendliness of health monitoring processes. Consequently, individuals will be able to closely monitor their health status and proactively detect potential health concerns.

- Sources: Ten-chip, temperature, acceleration, and PPG sensors.
- Activities: data processing including collection, transfer, visualisation, model development
- Roles: Sensor Manufacturers, Data Subjects (please find the definition of these roles at the beginning of this section)
- Data accessibility: Only the manufacturer can access all data.

Second data flow for initial clinical validation in the product development phase

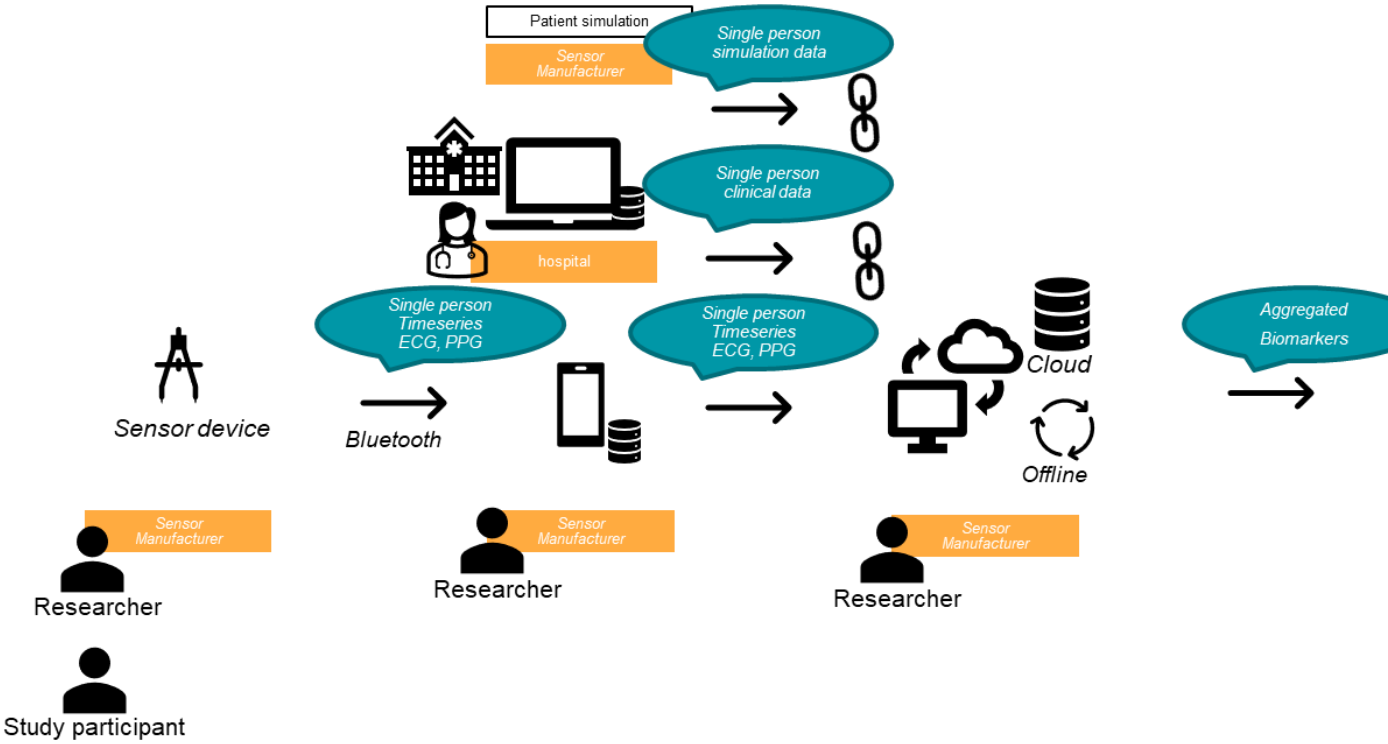

Figure 4 - Data flow for sensor device as an example pertinent to Product development

- Purpose: Initial clinical validation for the product development phase
- Sources: local memory of device that collects timeseries data from participants or transfers it via Bluetooth to a smartphone. The timeseries data comprises an electrocardiogram (ECG), a photoplethysmogram (PPG) obtained at the finger and tri-axial acceleration data from an inertial measurement unit (IMU). Subsequently, the data will be uploaded to the cloud. In addition, timeseries data will be downloaded from server to local computers for further processing.
- Activities: data processing including collection, transfer, transformation from timeseries signals to proxy values of blood pressure.
- Roles: Researchers of Sensor Manufacturer
- Data accessibility: Any corresponding clinical data, which will make the clinical trial participants identifiable, will remain with the clinical (principal) investigator of the clinical trial at all times. In contrast, the timeseries data will be downloaded from the server to local computers for further processing (e.g., transformation from timeseries signals to proxy values of blood pressure) by researchers. Ultimately, the processed (i.e., cleaned and transformed) data will be provided to specified consortium partners as aggregated biomarkers for AI model development towards novel metabolic syndrome biomarkers.

3.1.3 Reimbursement (D)

Reimbursement is the phase where clinical outcomes data is used to aid the economic analysis of solutions. Below you find a description of data flows pertinent to this phase (phase D in the development cycle), taking a platform of one of our Bio-curity partners to illustrate (see Figure 5).

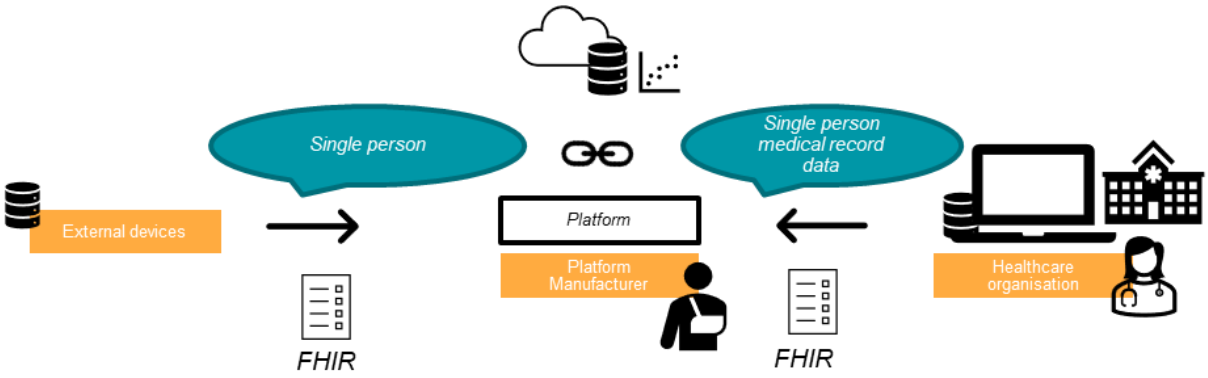

Figure 5 - Data flow for platform as an example pertinent to Reimbursement

- Purpose: Establishing the value and effectiveness of medical interventions and sensors developed in order to secure reimbursement from healthcare payers such as insurance companies or government agencies.
- Sources: Clinical outcomes data and economic analyses will be generated through rigorous research and trials. The data flow captures information about the effectiveness of the medical intervention and sensors in terms of patient outcomes, safety, and overall impact on healthcare delivery. Clinical outcomes data will be collected from various sources, including clinical trials, observational studies, patient records (EHRs), and real-world evidence (sensors).
- Activities: data processing including collection, transfer, visualisation, model development
- Roles: Researchers, Sensor manufacturers, Platform manufacturers, Healthcare practitioner (please find the definition of these roles at the beginning of this section)
- Data accessibility: Various stakeholders will need access to relevant data to evaluate the value, safety, and effectiveness of a medical product. In terms of data that can potentially identify individuals, it will be accessible to the healthcare providers with a strict patient privacy regulation to be followed (e.g., see the list presented in Section 2). Furthermore, ethics committees overseeing clinical trials and research studies might need access to identifiable data to assess the ethical considerations of the research. On the other hand, non-identifiable data will be accessible for parties reviewing clinical and economic data for reimbursement decisions and manufacturers that can share non-identifiable data in reimbursement submissions to support the product's value proposition.

3.2 Proposed Data Flow

Within the Bio-curity project, the goal is to develop digital biomarkers that can track the health of patients in real-time. This would be a revolutionary step towards preventive and predictive medicine, allowing health care providers to advise their patients to reduce risks of certain conditions or intervene timely with treatment. However, monitoring patients in real-time raises serious security and privacy

concerns. Where is this sensitive information about a patient stored, and who has access to this sensitive information?

To address these concerns, not only must it be clear who has access to which data, the patient must also be able to control who has access to which data. If a patient decides that for whatever reason, he or she no longer wishes that a doctor receives their real-time vitals, the technology should allow changing this. It should be up to the patient to decide with whom to share data, when to start, and when to stop. We call this concept "patient in control".

A recent technological development that implements this concept is Self-Sovereign Identity[3]. By itself, the core idea of Self-Sovereign Identity is that the internet misses an identity layer. On the internet, one has no idea who one is talking to on the other end of the line, which makes it impossible to digitally establish trust. There are methods around this limitation, like logging into a website through an "Identity Provider" which creates and manages digital identities to authenticate users or provide authentication services to third parties (such as "Login with Google/Facebook/…" button). However, these solutions are far from perfect. Self-Sovereign Identity is an alternative approach in which users have a decentralized identity. These decentralized identities allow claims made about such an identity to be *verifiable*. A user can collect verifiable claims about its identity from (authoritative) sources and choose to share these with other parties.

Another concept to consider when designing new data exchanges is to ensure that the data is *fit for purpose*. A key element of the Qualified Data Exchange model is to take a bottom-up approach when it comes to describing the criteria of specific instantiation of a data exchange to ensure this. A data exchange has a purpose, and thus the data required in the exchange should match the needs of the purpose. Not only does this mean the data is in the correct format and there exists semantic interoperability, but also that the data has the correct *assurances*. For example, a web shop and a bank might both request a user's name, yet the bank needs a much higher level of *assurance* about the validity of this piece of information. So, when two parties communicate, not only does it need to be decided what the communicated data looks like (its syntax and semantics), but also under which conditions the data is regarded *valid for its purpose*.

As described in the methodology, we first take a bottom-up approach in reasoning about the criteria for the Bio-curity project. In this section specifically, we explore some preliminary design choices with impact on the technology architecture. These are not yet final and instead serve as input for designing the final technology architecture.

Decision 1: Data exchange between Sensor and Sensor Provider

As has been described in Section 3.1 on the current dataflows, the data generated by sensors on the patient must first be sent to the sensor provider for processing.

For existing sensors deployed in the reimbursement phase, the status quo is to let the sensor on the patient freely send all its data to the sensor provider. This has the benefit that the data is transformed by the sensor provider in human readable and interpretable form without any user interaction. The main downside of this approach is that the real-time health information about the patient is now sent

[3] Self-sovereign identity: managing data safely | TNO

to and stored at the sensor provider, even though the sensor provider has no need for health information on specific patients.

The alternative is to share this data through the user. The sensor data collected about the user can be naturally seen as owned by the user. This data could be collected by the user via the smartphone. The user would then be free to share this data with any party that provides services based on such sensor data.

One possible problem with this approach is that the sensor data of the sensor providers might constitute intellectual property, and as such could not be shared to the user in plain. Another potential issue is that of the user experience. If the sensor must store its data in a user-controlled storage, an additional setup step is required by the patient compared to a sensor that has its own connectivity built-in.

Decision 2: Data exchange between Sensor Provider and Platform Provider

The second decision to make is how the information about the patient will flow from the sensor provider to the platform provider. The choice here again is whether to send this data via the user. The traditional approach would be to send the data from the sensor provider directly to the platform provider, provided the patient has consented to this exchange. This approach has the downside of requiring all sensor and platform providers to be able to exchange data with each other, and relies on proper consent management by the providers. Alternatively, the sensor provider may share the processed sensor data with the user, who in turn shares this data with the platform provider. This introduces the patient as a single point of interoperability, and more concretely links consent to data sharing, as the patient decides when and what to share.

Decision 3: Sensor Data Processing at Home

In the previous two sections, it is assumed that the raw sensor data is sent to the sensor providers for processing. To fully place the patient in control and minimize the amount of data shared with third parties, the ideal scenario would be to do the processing locally on the users' devices. The obstacle for this approach, however, is that the processing algorithms must be able to run on low-power devices, such as the mobile phone of the patient.

4. Security and assurance

4.1 Analysis of Risks

Risk assessment plays a pivotal role in shaping the development of security and assurance criteria for the intended trust model within the Bio-curity project. In the context of data protection and privacy within Bio-curity, a risk-based approach that involves assessing the potential risks to personal and health data and implementing appropriate measures to manage and mitigate those risks has been already described in D1.2 *Data protection and privacy guidelines*, that serves as an input for this deliverable. By understanding the specific risks and challenges, the project team can now make informed decisions to design a robust and effective trust model that adequately mitigates those risks.

For The Netherlands inside the MedMij framework the OWASP guidelines are mandatory[4]. Within these guidelines they present this risk assessment.

The link between risk analysis and assurance criteria for the intended trust model is fundamental and inseparable. Risk analysis informs the development of security and assurance criteria, ensuring that the trust model is designed to effectively address identified risks and mitigate potential threats. The process of risk analysis and the subsequent security and assurance criteria work together in a cyclical manner to create a robust and trustworthy system. Here's how they are connected:

1) **Risk Identification**: Risk analysis involves identifying potential threats, vulnerabilities, and weaknesses in the intended trust model. These risks arise from various sources, including technical vulnerabilities or malicious actors attempting to exploit the system. The identification of risks provides the basis for determining the specific security and assurance requirements that the trust model needs to meet. The identified risks can be all seen in detail in D1.2. The paragraph below presents the brief outline of the main recognized risks that are being used and implemented in defining criteria and components for the intended trust model:

Risk	R01: Unauthorized Access
Threat	Unauthorized individuals accessing personal information, leading to data breaches and malicious activities.
Risk	R02: Data breaches
Threat	Unauthorized access, disclosure, or theft of sensitive data, resulting in financial loss and reputational damage
Risk	R03: Inaccurate or Incomplete Data
Threat	Relying on incorrect or incomplete data leading to flawed analysis and decision-making.
Risk	R04: Profiling and Discrimination
Threat	Unfair targeting or discrimination based on personal characteristics, posing ethical and legal concerns.
Risk	R05: Loss of Control Over Personal Data
Threat	Unauthorized access or misuse of personal data, risking data breaches and privacy violations.
Risk	R06: Secondary Use of Data
Threat	Personal data used for unintended secondary purposes without consent.
Risk	R07: Data Loss
Threat	Permanent data loss due to system failures or errors.
Risk	R08: Consent Mismanagement
Threat	Failure to obtain or manage proper consent for data processing.
Risk	R09: Insecure Data Storage
Threat	Unauthorized access, breaches, or loss due to inadequate data storage security.
Risk	R10: Insecure Data Processing
Threat	Unauthorized access or improper handling of data during processing.

[4] OWASP Risk Rating Methodology | OWASP Foundation

2) **Risk Evaluation**: After identifying risks, they have been evaluated to understand their likelihood of occurrence and potential impact on the system and its users (*based on the Risk assessment matrix, see Figure 1*). The risk evaluation approach should consider the most affected party, as this approach ensures that the highest potential impacts are adequately managed and mitigated. This evaluation helped to prioritize risks based on their severity and guides the allocation of resources towards the most critical areas of concern. Risks with high likelihood and significant impact may require more stringent security measures and assurance mechanisms.

5x5 matrix	IMPACT How severe would the outcome be if the risk occurred?				
LIKELIHOOD What is the probability the risk will happen?	1 (Insignificant)	2 (Minor)	3 (Moderate)	4 (Major)	5 (Severe)
5 (Extreme or Highly Likely)	Moderate	Moderate	High	Critical	Critical
4 (Major)	Low	Moderate	Moderate	High	Critical
3 (Medium or Possible)	Low	Moderate	Moderate	Moderate	High
2 (Low or Unlikely)	Very Low	Low	Moderate	Moderate	Moderate
1 (Negligible or Rare)	Very Low	Very Low	Low	Low	Moderate

Figure 1. Risk assessment matrix

3) **Security and Assurance Criteria Development**: Based on the results of the risk analysis from D1.2, security and assurance criteria can be formulated. These criteria outline the specific security controls, protocols, and practices that will be implemented to mitigate identified risks effectively. The criteria are tailored to address the vulnerabilities and threats identified during the risk analysis process.

4) **Risk Mitigation**: The security and assurance criteria aim to reduce the likelihood of risk occurrence and minimize the impact of potential incidents. By incorporating appropriate security measures, such as encryption, access controls and regular data backups, the trust model can be fortified against potential threats. Assurance mechanisms, such as auditing, monitoring, and compliance checks, further enhance the system's resilience and reliability.

5) **Iteration and Improvement**: The process of risk analysis and the development of security and assurance criteria are iterative. As new information emerges, and the threat landscape evolves, the risk analysis should be revisited to identify any changes in the risk profile. The security and assurance criteria then must be adjusted accordingly to adapt to new risks and challenges.

The identified risks in the Bio-curity project are interlinked and form the foundation for establishing robust security and assurance criteria. These risks encompass unauthorized access, data breaches, inaccurate data, profiling, loss of data control, and many more. Addressing these risks through measures like strong authentication, encryption, data minimization, clear consent processes, and comprehensive data documentation ensures the project's security, privacy, and ethical integrity, thus defining the project's overarching security and assurance criteria.

In summary, risk analysis provides the foundation for the development of security and assurance criteria in the intended trust model. It ensures that security measures and assurance mechanisms are tailored to address identified risks, thus creating a robust and trustworthy system that instils confidence in its users. The iterative nature of this link ensures that the trust model remains adaptable and effective in the face of evolving threats and challenges.

4.2 Criteria derived from laws, regulations and standards

The criteria for security and assurance of the envisioned Bio-curity platform are formed by relevant themes which emerged for the thematic analysis. Relevance was ensured by: 1) the selection of regulations and technical standards (our corpora) crafted to the themes of the project; and 2) filtering through themes and assigning them to at least one component or party involved in the platform: the data itself (4.2.1), the people whom the data is about (4.2.2), the exchange of data between providers (4.2.3), the platform as a whole (4.2.4) – these map into the categories of criteria we present below.

Two other categories emerge for themes that appear consistently, but are considered out of scope as they are in the fringe of our envisioned Bio-curity platform: Healthcare and Health Ethics (4.2.5), although these are criteria of undoubted importance, they are only relevant for some partners in the project; and Automated processing (4.2.6), which similarly is not present in all platform or sensor providers. We present them in this report for the sake of completeness.

Terminology differs according to the domain of each regulation and standards reviewed. In several cases we refrain from changing the original terms, instead we adopt the following understanding:

- Data, personal data, electronic health record, file, health data: data collected, processed (in the broad interpretation of the term, see GDPR, Article 4(2)), shared about a person.
- Data subject, patient, user, study participant: the person who the data is about.
- Controller, data holder, organization: legal entity which collects and processes data, and is accountable for it.
- Third party, data recipient: other entities (legal or natural persons) which partake in joint processing or data exchange.
- System, product, service: designates the variety of software-hardware combination provided by Bio-curity partners, which interfaces with natural persons.

- Platform: the envisioned Bio-curity qualified data exchange platform for which criteria are devised.

In what follows we present the comprehensive set of criteria, organised by categories, and inside each category presented in descending order of frequency of appearance in our corpora. The description found here is a summary of the contents found under each criterion, for a full list of quotes and references, please see D4.1 Appendix.

4.2.1 Data Management and Quality

Category comprising the group of criteria concerning ensuring and maintaining quality of data, including its content and metadata.

Theme	Criteria
Identification	Data is stored in a way that permits identification when confirmation of identity is necessary.
Data format	Platform supports description of data format. Including, but not limited to: types and formats of electronic health data, metadata, support documentation, data model, data dictionary, standards used, provenance, nature and volume likely to be generated, data structures, vocabularies, classification schemes, taxonomies, code lists, whether data is likely to be generated continuously and in real-time.
Data permit	Platform supports the use of data permit which sets out conditions applicable to the processing of data when data is exchanged between parties.
Data description	Platform supports description of data. Including, but not limited to: data source, geographical coverage, representation of multi-disciplinary electronic health data, representativity of population sampled, average timeframe in which a natural person appears in a dataset, time between collection of data and their addition to the dataset, time to provide data following a data access application approval, data enrichments, merging and adding to an existing dataset, links with other datasets, dataset content, use restrictions, licenses, data collection methodology, data quality and uncertainty.
Interoperability	Platform facilitates data interoperability.
Data governance	Platform supports governance of data. Including, but not limited to: ensuring the processing period is not exceeded, extending the period when necessary, conducting regular audits, maintaining and making available a metadata catalogue of datasets.
Data quality	Platform supports description of data quality. Including, but not limited to: technical quality, showing completeness, uniqueness, accuracy, validity, timeliness, consistency of data, data preparation processing operations, such as annotation, labelling, cleaning, enrichment, aggregation, formulation of relevant assumptions, identification of gaps or shortcomings.
Data source	Platform supports description of source from where data originates, and whether they come from publicly available sources.
Data anonymization	Data is in an anonymized format whenever the purpose of processing can be achieved with such data, or identification is no longer necessary.
Data accuracy	Data is accurate.

Data management	Platform supports data management. Including, but not limited to: keeping records of processing activities, maintaining systematic and orderly policies, procedures or instructions for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data.
Data access application	Platform supports the use of data access application which describes the data needed, intended use and the purposes for processing of data when exchanged between parties.
Data quality management	Platform supports the description of data quality management. Including, but not limited to: level of maturity of data quality management process, review and audit processes, biases examination.

4.2.2 Rights and Interests of Data Subject

Category comprising the group of criteria describing the rights and interests of people whose data is processed, as described in regulations and standards.

Theme	**Criteria**
Information to be provided	Information is provided on, but not limited to: examination and treatments, action taken upon request (to execute rights), identity and contact of controller, processing purposes and legal basis, when applicable the legitimate interest, intention to transfer data to a third country, whether there is an adequacy decision, appropriate safeguards for the transfer, retention period of data, the right to withdraw consent at any time, the source of data, existence of automated decision-making, underlying logic, importance and expected consequences of it, envisaged sharing of data, recipients of personal data, the nature and volume of data likely to be generated, whether data is generated continuously and in real-time, how to access data, means of communication to contact the data holder, who viewed or requested (part of) data, and on which date, and the circumstances in which cryptography is used to protect data.
Purpose limitation	Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. A health insurer does not have access to electronic exchange systems. A third party shall not make the data it receives available to another third party (in raw, aggregated of derived from) unless necessary for the performance of a contract or agreed upon service, or use the data to develop a competing product or system. Personal data is not used for testing, synthetic data may be used instead.
Right to be informed	Platform supports the right to be informed about, but not limited to: the purpose for (and prior to) further processing data, confirmation as to whether personal data of a specific person is processed, appropriate safeguards applicable to international transfer of data, lifting of restriction of process, healthcare providers and professionals that have accessed data, residual risks of AI systems, and data breaches.

Right to data access	Platform supports providing the data subject with access to or a copy of the personal data being processed, in a commonly used electronic format.
Erasure of data	Platform supports erasure of data without undue delay, upon request or when data is no longer needed for the identified purposes.
Data portability	Platform supports transmitting data in a structured, commonly used and machine-readable format, to another controller.
Rectification of data	Platform supports rectification of inaccurate data, and the completion of incomplete data upon request.
Rights and interests of others	Rights and interests (e.g., access to data, erasure, and restriction of processing) take place only to the extent that they do not harm the rights and interests of others, in particular vital interests.
Information about rights	Information is provided clearly and separated from other matters, about the existence of the following rights, including how to execute them: access, rectification, erasure of data, restriction of processing, objection to processing, data portability, sharing data, and to lodge a complaint with the competent authorities.
Right to object to processing	Platform supports objection to processing and ceases it unless compelling legitimate grounds for processing can be demonstrated, which override the interests, rights and freedoms of the data subject.
Restriction of processing	Platform supports restriction of processing when the accuracy of personal data is contested, for a period that enables the controller to verify it.
Storage Limitation	Platform does not retain personal data for longer than necessary for the purposes of processing.
Right of minors	Obligations towards minors are fulfilled towards a fiduciary (parents, guardian, representative who exercises authority over the minor). Minors receive information adapted to their age.
Rights to share data	Platform supports transmitting data to a recipient of choice and sharing data with a third party.
Right to restrict access	Platform supports restriction of access of health professionals to all or part of electronic health data. The professional shall not be informed of the existence and nature of the restricted data.

4.2.3 Information Security

Category comprising the group of criteria necessary to ensure secure data exchange between Sensor and Platform Providers.

Theme	**Criteria**
Security measures	Platform supports adoption of technical and organizational measures to ensure an environment with level of security appropriate to the risk. Including but not limited to: pseudonymization and encryption of data, ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services, restoring availability and access to personal data in a timely manner in the event of incidents, regularly testing, assessing and evaluating the effectiveness of measures to ensure security of processing, protection against unauthorized access, copying, modification or removal of

	data, protection and encryption of network communications, encryption of communication channels, and keeping identifiable logs of access for auditing purposes.
Legal basis	Platform ensures there is a legal and valid basis for processing and sharing of data and supports its documentation.
Confidentiality	Platform ensures confidentiality (prevent sensitive information from unauthorized access attempts) of data by: ensuring no health information about a patient is provided to or accessed by others without patient's consent, data exchange is secured along the entire path between sender and receiver, data is encrypted prior to exchanging, protecting against unauthorized access or unlawful processing, protecting commercially confidential information, trade secrets, and intellectual property rights.
Access control	Platform adopts an access control system that allows: granular rules to represent different categories of electronic health record required by different health professionals, restriction of data access to authorized parties, overrule of restrictions to protect vital interests of people.
Authorized access	Access to data may be granted to authorized parties, or authorized without patient's consent for statistics or scientific research in the field of public health if requesting permission is not reasonably possible, and the privacy of patients is not disproportionally harmed, or if data is anonymized.
Data transfer	Platform supports data transfer to third parties, international organizations or to third countries with appropriate and suitable safeguards.
Integrity	Platform ensures integrity of data (maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle) by protecting it against accidental loss, destruction or damage, and against forgery.
Encryption	Encryption is used to safeguard rights and freedoms of natural persons where anonymization may significantly affect the purpose pursued.
Safeguards	Platform supports the implementation of safeguards to protect rights and legitimate interests of data holder and concerned natural persons.
Logging	Platform supports logging of user activities, exceptions and information security events, their regular review, and ensures logs are protected against forgery and unauthorized access.
Pseudonymization	Pseudonymization (de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers) is used to safeguard rights and freedoms of natural persons where anonymization may significantly affect the purpose pursued. The information necessary to reverse pseudonymization is only available to authorized parties, and failure to respect pseudonymization is subject to penalties.
Robustness	Platform contains components of automated processing with high degree of robustness to avoid functional errors and to withstand manipulation by third parties.
Availability	Platform ensures availability (accessibility by authorized parties consistently and readily) of processing systems and services.

4.2.4 Transparency and Accountability

Category comprising the group of criteria concerning building and maintaining trust between people and the Bio-curity platform.

Theme	Criteria
Consent management	Platform supports consent management by: establishing and documenting a process by which it can demonstrate whether, when and how consent to process data has been obtained, requesting (where appropriate, in written form and dated) and keeping record of explicit permission to process data for a specific purpose, and allowing easy withdraw of consent at any time. Additionally, supporting information of expected consequences and risks to the health of the patient in case proposed examination, treatment or procedures are not performed.
Accountability record	Platform supports record keeping in written form of the processing activities containing: name and contact of controller(s), processor(s), any joint controllers, representatives (or Data Protection Officer), processing purposes, categories of data subjects, categories of personal data, categories of (envisaged) recipients including in third countries and international organizations, and retention period of different categories of data.
Accountability	Platform supports accountability of controllers, facilitating the demonstration of compliance with regulations and standards.
Data minimization	Platform supports data minimization by ensuring personal data is adequate, relevant and limited to what is necessary for the purposes for which they are processed.
Communication	Communication with patients is guided by what they should reasonably know and is appropriate to their comprehension. Communication with any natural person is presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.
AI monitoring	Platform supports logging capabilities that enable the monitoring of AI systems operation, including the continuous monitoring of risks and serious incidents. Additionally, supporting the logging of events regarding AI systems in a recognized standard or common specification.
Oversight	Platform supports human oversight of AI systems to do the following, as appropriate to the circumstances: duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible, remain aware of the possible tendency of automatically relying or over-relying on the output produced by the AI system, and be able to correctly interpret the AI system's output.
Transparency	Personal data is processed in a transparent manner. AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable interpretation of the system's output and its appropriate usage.
Auditability	Platform facilitates the inspection of personal data, including health data, and transactional data by authorized parties.

Proportionality	Processing of data follows the principle of proportionality with respect to the identified purposes.

4.2.5 Healthcare and Health Ethics

Category comprising the group of criteria concerning building and maintaining trust between people and Healthcare providers.

Theme	Criteria
Electronic Health Record	Platform supports recording of data concerning health of patients and everything necessary for their proper care in a file. Additionally, other information is noted in the file: regarding provision of data without the patient's consent, citizen service number for identification, and information inserted by the patients themselves.
Ethical conduct	The care provider withholds information from the patient about proposed examination, treatment or procedure insofar as providing it would cause serious harm to the patient. The information is provided as soon as the harm is suspected to be no longer applicable. No incentives or financial inducements are given to subjects of clinical trial or their legal representatives.
Accessibility	Platform facilitates access to at least the priority categories of electronic health data by health professionals through health professional access services. Health professionals have access to the electronic health data of natural persons under their treatment, irrespective of the Member State of affiliation and the Member State of treatment.
Doctor-patient confidentiality	Personal data is to be kept confidential for reasons of professional secrecy, office, or agreement.
Protection of vital interests	Processing of data is lawful if it is necessary to protect the vital interests of the data subject or another natural person.

4.2.6 Automated Processing

Category comprising the group of criteria concerning rights and obligations related to automated processing of personal data.

Theme	Criteria
Smart contracts	Smart contracts may be used as technical protection measure to prevent unauthorized access to data and are protected themselves through rigorous access control mechanisms at the governance and smart contract layers. Such technical protection measures shall not be used to hinder the user's right to effectively provide data to third parties.
Automated decision-making	Automated decision-making, such as profiling, is subject to special rights (e.g., to object) and obligations (i.e., provision of information about it).
AI risks	AI systems are continuously and iteratively subject to risk management consisting of, but not limited to: identification and analysis of risks, estimation

	and evaluation of risks that may emerge with the use of AI systems, evaluation of risks based on data analysis gathered from post-market monitoring.
Safe termination and interruption	Automated processing can be safely terminated or interrupted, as appropriate to the circumstances.
Overrule	A person in charge is able to decide, in any situation, not to use the AI system or otherwise disregard, override or reverse its output.
AI bias	AI systems are examined and monitored in view of possible bias.
AI vulnerabilities	AI systems are resilient against attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities. Specifically, attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.

4.2.7 Other emerging themes

Other relevant themes emerged from our thematic analysis that do not fit to any part or component of the envisioned Bio-curtiy platform. We list them below.

- **Compensation** – in different regulations compensation is made optional (European Health Data Space, Article 3(8)), or authorized only in case of loss of earnings directly related to the participation in a clinical trial (Regulation on Medical Devices, Article 64(1) and 65(1)).
- **Retention** – retention of data is mentioned in several regulations and standards and incorporated in the criteria presented above. However, only in one case a specific period of minimum 20 years after the last change to the file is mentioned (Wet op de geneeskundige behandelingsovereenkomst, Article 454(3)). We refrain from using this minimum period in our criteria as it is specific to health treatment in the Netherlands.
- **Fiduciary** – in several regulations the role of a fiduciary is mentioned under specific circumstances. Normally in case the data subject is a minor, or incapacitated. Fiduciaries can be parents of a child, guardians, legal representative, or a person that exercises authority over another, towards whom obligations are fulfilled and rights are granted.
- **Age restrictions** – in several health-related regulations we encountered rules conditioned or restricted to the age of the patient/subject. Where applicable we include them in the criteria above (e.g., communication is appropriate to the patient's comprehension). However, in different scenarios the restrictions apply to different ages, such as age of 12 (Wet op de geneeskundige behandelingsovereenkomst, Article 448(1), 465(1)), and ages between 12 and 16 (Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg states in Article 15g). Therefore, we refrain from suggesting a specific number when age restrictions appear in our criteria.

5. Discussion and Conclusion

As shortly introduced in our 'Context' section, we took the QDX model as a guide for our research on security and assurance criteria for a qualified data framework. Following its bottom-up approach, we initiated our investigation by interviewing partners interested in data exchange (including questions

like 'What is the purpose of the data exchange? What kind of assurances do they need in order to make the data 'valid' for their purpose?). However, at this early project stage, definitive answers were lacking due to ongoing development. Consequently, we transitioned to an operational level, examining the current data flow for tangible instances and exploring the underlying rationales. This exploration informed us on the themes and roles to take into consideration for our future trust model, that will be the basis for our Bio-curity platform.

The elicitation of criteria on the other hand was realized following a top-down approach. This was done in reaction to the early stage the project is currently: ideas for data exchange are still in the development phase and still need to be matured. What emerged from the discussions with consortium partners (Sensor and Platform manufacturers) are general concerns with *data quality and managemen*t, and *data protection*.

We derive criteria through a thematic analysis, departing from regulatory framework and technical standards (our corpora) related to healthcare and the processing of health data. We do not claim completeness of our corpora, mostly due to the fact that it was decided among the consortium partners to exclude Turkish regulations (as European regulation is more stringent). Even considering only European regulations and standards, these can be further specified by member states, and only those relevant to the Netherlands were analysed. However, we have reasons to believe the criteria emerging from our thematic analysis are complete. As topics repeat across several documents, even if our corpora miss some sources, we believe relevant topics likely appear in one (or multiple) of the reviewed documents.

The validity of our criteria cannot be guaranteed from our methodology alone, since it does not depart from the real needs of consortium partners. Although the criteria are relevant to the topic (because they are selected from relevant corpora) they might not be fit for the purpose which partners *need* and *desire* to exchange data.

To investigate if the criteria are fit-for-purpose we propose two tests: 1) fitness of our criteria towards the needs of partners can be tested against the elicited risks, these were collected form the partners independently of this work, and can provide a source for validation more aligned with the bottom-up approach; and 2) fitness of our criteria towards the desires of partners can be tested by requesting input from partners, mostly for the prioritization of criteria, because our list is comprehensive we believe it is likely to cover desires too, but they are likely mixed with other less urgent criteria. While the latter test will be a subject of our next deliverable, the former was already conducted by the team.

The ten risks identified by Bio-curity consortium in D1.2 are assessed according to their likelihood and severity, leading to a risk score. For each risk a mitigation plan is proposed. To test the fitness of our criteria we select the ones with a risk score of "high" or higher (see 4.1), and for each identified mitigation strategy we map them onto the relevant criteria we identified. Because we found links covering, at least partially, every high scoring risk, we deem our criteria valid towards the needs of consortium partners. We note however, that criterium "Security measures" appears often, and it remains future work to investigate the appropriate granularity for this criterium.

Table 1 below shows a summary of this analysis, for a full description of risks, please refer to D1.2.

Table 1 - Validation of criteria based on risks and identified mitigation strategies

Risk	Mitigation strategy	Criteria
R01 – Unauthorized access	Authentication mechanisms	Security measures
	Regular updates and patch systems	Security measures
	Secure network connections	Security measures; Encryption; Integrity; Confidentiality
	Access controls	Access control; Security measures
	Monitor and log activities	Logging; Security measures
R02 – Data breaches	Data classification	-
	Access controls and user authentication	Access control; Authorized access
	Encryption	Encryption; Confidentiality
	Regular data backups	Availability; Security measures
	Compliance with regulations	Accountability; Accountability records
R05 – Loss of control over personal data	Data minimization	Data minimization
	Informed consent	Consent management; Information to be provided
	Data security measures	Security measures; Access control; Authorized access; Encryption; Confidentiality
	Data subject rights	Entire category for rights and interests (4.2.2)
R07 – Data loss	Regular data backups	Availability; Security measures
	Data encryption	Encryption; Confidentiality
	Access control and authentication	Access control; Authorized access
R09 – Insecure data storage	Strong data encryption	Encryption; Confidentiality
	Access control	Access control; Security measures
	Multi-factor authentication	Security measures
	Data segregation	-
R10 – Insecure data processing	Data encryption	Encryption; Confidentiality
	Secure data transmission	Data transfer; Security measures
	Secure development practices	-
	Data minimization	Data minimization
	Access control and authentication	Access control; Authorized access
	Data anonymization and pseudonymization	Data anonymization; Pseudonymization

6. References

Joosten, R. (2023). *Qualified Data Exchange: An introduction.* TNO.

MedMij. (2023, August). *Juridish kader*. Opgehaald van https://afsprakenstelsel.medmij.nl/display/MMOptioneel/Juridisch+kader

NEN. (2017). *NEN 7510-1 Medische informatica - Informatiebeveiliging in de zorg - Deel 1: Managementsysteem.*

NEN. (2017). *NEN 7510-2 Medische informatica - Informatiebeveiliging in de zorg - Deel 2: Beheersmaatregelen.*

NEN. (2018). *NEN 7513 Medische informatica - Logging - Vastleggen van acties op elektronische patiëntdossiers.*

NEN. (2021). *NEN-EN-ISO/IEC 27701 Veiligheidstechnieken - Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiemanagement - Eisen en richtlijnen.*

NEN. (2022). *NEN 7512 Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling.*

Nowell, L. S. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods, 16(1)*.

Roche Information Solutions in collaboration with Prova Health. (2023). *Generating evidence for digital health solutions.* Rotkreuz: Roche Diagnostics International Ltd.

[i] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

[ii] Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg - wetten.nl - Regeling - Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg - BWBR0023864 (overheid.nl)

[iii] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) [2022] COM/2022/68 final - EUR-Lex - 52022PC0068 - EN - EUR-Lex (europa.eu)

[iv] Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space [2022] COM/2022/197 final - EUR-Lex - 52022PC0197 - EN - EUR-Lex (europa.eu)

[v] Wetvoorstel 35.824 voor Wet elektronische gegevensuitwisseling in de zorg - Wet elektronische gegevensuitwisseling in de zorg (35.824) - Eerste Kamer der Staten-Generaal

[vi] Burgerlijk Wetboek Boek 7 Afdeling 5. De overeenkomst inzake geneeskundige behandeling - wetten.nl - Regeling - Burgerlijk Wetboek Boek 7 - BWBR0005290 (overheid.nl)

[vii] Wijzigingswet Wet cliëntenrechten zorg, enz. (taken en bevoegdheden op het gebied van de kwaliteit van de zorg) - wetten.nl - Regeling - Wijzigingswet Wet cliëntenrechten zorg, enz. (taken en bevoegdheden op het gebied van de kwaliteit van de zorg) - BWBR0034672 (overheid.nl)

[viii] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1

[ix] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS [2021] COM/2021/206 final