Ref. Ares(2022)1935168 - 16/03/2022

ICT-56-2020 "Next Generation Internet of Things"
Grant Agreement number: 957218

IntellioT

# Deliverable D1.6
# Data de-identification procedures and tools

| | |
|---|---|
| Deliverable release date | 31/12/2021 |
| Authors | 1. Anca Bucur, Nancy Irisarri Méndez (PHILIPS)<br>2. Maria Marketou, Ioannis Anastasiou (PAGNI)<br>3. Konstantinos Fysarakis (SPHYNX) |
| Editor | Nancy Irisarri Méndez (PHILIPS) |
| Reviewer | Beatriz Soret (AAU)<br>Sumudu Samarakoon (UOULU) |
| Approved by | PTC Members: (Vivek Kulkarni, Konstantinos Fysarakis, Sumudu Samarakoon, Beatriz Soret, Arne Bröring, Maren Lesche)<br>PCC Members: (Vivek Kulkarni, Jérôme Härri, Beatriz Soret, Mehdi Bennis, Martijn Rooker, Sotiris Ioannidis, Anca Bucur, Georgios Spanoudakis, Simon Mayer, Filippo Leddi, Harshitha Chandregowda, Maren Lesche, Georgios Kochiadakis) |
| Status of the Document | Final |
| Version | 1.0 |
| Dissemination level | Public |

# Table of Contents

# 1 INTRODUCTION

This deliverable reports on the chosen methodology for privacy assurance and de-identification of data from patients enrolled in the pilot study conducted in the context of healthcare use case (UC2) of the IntellIoT project, on the procedures that have been implemented for de-identification, and on the assessment of the outcomes of the de-dentification (including privacy and re-identification risk assessment). We also describe the data life cycle with the main data processing that we will perform. A description of the privacy and security measures employed in the IntellIoT project is also included, as they relate to data processing.

# 2 DATA LIFE CYCLE

This section describes the flow of data through several processing steps that will be performed in order to use the data for research and analytics by members of the IntelIIoT consortium and for analysis by physicians.

## 2.1 Collection

Patient data collected in IntelIIoT is provided by the participants on a voluntary basis, in accordance with well-defined informed consent procedures, goals of data processes and individual's rights, pursuant to the relevant principles of the General Data Protection Regulation (GDPR). All patients whose data will be processed in the context of the IntelIIoT project will have provided written informed consent for participation and use of the data for the purposes of the project, according to the Good Clinical Practice (GCP) principles. Informed consent procedures, as well as pilot study design, are described more comprehensively in deliverables D1.3 and D1.4.

More details on the data collection are provided below.

I. Types of data to be collected at the time of patients' enrollment in the project include:

A) Patients' demographic and physical characteristics:

-Personal information (name / surname);

-Gender;

-Date of birth;

-Height and weight.

B) Medical Information:

-Comprehensive medical history, including medications;

-Vital signs: blood pressure, heart rate, oxygen saturation;

-Data regarding findings of baseline clinical examination;

-Electrocardiogram (ECG), echocardiogram and blood tests results (routine clinical practice).

II. Types of data to be collected prospectively after patients' enrollment include:

A) Information of patients' clinical course (standard-of-care):

-Data regarding findings of clinical examination at each scheduled clinical reassessment;

-Changes in medications and adherence data;

-Adverse events (vital status, hospitalizations, unscheduled healthcare encounters, changes in symptoms / functional capacity);

-Results of repeat diagnostic / follow-up testing (ECGs, echocardiographic studies, blood tests);

-Quality-of-Life questionnaires.

B) High-volume digital data from measurements of biological parameters collected from smart devices (smartphone, smartwatch, weight scales, pulse oximeter, blood pressure monitor, thermometer):

-Heart rate, ECG tracings, blood pressure, oxygen saturation, body weight / body composition details, body temperature, physical activity data.

III. Data Minimization Principle:

In accordance with the Data Minimization Principle, only adequate, relevant, and limited personal data that is necessary for the proper conduct of the IntelIIoT project will be collected and processed.

IV. Data collection process:

A) Types of data outlined in sub-sections IA, IB and IIA of section 2.1 of the present document will be collected:

-Directly from the enrolled patients (medical history, previous examinations);

-Directly from the medical records kept at University General Hospital of Heraklion (PAGNI) and electronic records / databases routinely accessible to physicians (such as electronic prescription records and hospital admission records).

These data will be kept in both paper and electronic files that will be safely kept at the Clinical Studies office of the Cardiology Department of PAGNI and will only be accessible to the physicians involved in the conduct of the IntelliIoT project.

Data will also be entered manually into a dedicated electronic file in the interactive IntelliIoT project platform (SharePoint) accessible to partners involved in the Healthcare Use Case of the IntelliIoT project; however, any data entered on SharePoint will be pseudonymized (each patient will have been allocated to a unique project ID not related to his/her name). This will follow the methodology described in Section 3 for the removal of direct identifiers and on transformation of quasi-identifiers. Any paper documents or electronic files including enrolled patients' name/surname or any other details that could reveal enrolled patients' identity will be securely kept (locked room / password protection) at the Clinical Studies Office of the Cardiology Department of PAGNI and will only be accessible to the physicians involved in the conduct of the IntelliIoT project and monitoring / regulatory authorities.

B) Types of data outlined in sub-section IIB of section 2.1 of the present document (device-derived data) will be collected and stored in a dedicated Patients Data Repository, which will be a server located at the IT department of PAGNI. Data stored in the repository will be accessible to delegated physicians (PAGNI) eponymously (i.e., name / surname will be visible) -for patients' safety reasons- via a dedicated password-protected platform (each physician involved in the project will be allocated a unique access code).

In parallel, data stored in the repository will be accessible to other IntelliIoT partners responsible for data processing, but only in a pseudonymized manner (i.e., all other partners involved will only have access to the unique project ID of each patient, and not on his/her name / surname).

All data categories listed above will be used for both clinical and research purposes. The sources of data from the sensors and human input employed in the IntelliIoT framework has been described in Deliverable 3.3 Sections 4.1.1.2 and 4.1.2.2, respectively.

## 2.2 Processing

Pursuant to Article 5 (Principles relating to processing of personal data) and Article 6(1)(a) of the GDPR (i.e., the data subject has given consent to the processing of his or her personal data for one or more specific purposes), any personal data which is processed in IntelliIoT is adequate (i.e., sufficient to properly fulfil the Project's stated purpose), relevant (i.e. has a rational link to that purpose), and limited to what is necessary (i.e., the Project does not hold more than what is needed for that purpose).

In more detail, the IntelliIoT project will process data to develop and evaluate the overall environment, its components, and analytical models. We will process data within two workflows.

During system development, collected data will be used to develop, integrate, and test the components and to train the proposed AI models within the federated learning solution described in Deliverable 3.2. A limited amount of data will be aggregated in a centralized fashion to train the base model. Additional data will be used to refine and evaluate the base model across mobile devices, without moving data from the patient environment, according to the federated learning approach.

A second workflow will drive the deployment phase of the IntelliIoT environment and the inference phase of the analytical models. In this workflow, data will be used to evaluate the integrated infrastructure and the developed models. Based on the collected data, the system will provide advice and recommendations to the patients and will interact and provide information to the clinicians (human-in-the-loop) to enable them to guide the patients. This is as well the evaluation phase in which we will assess the potential benefits of the system.

## 2.3 Disclosure

Results of the pilot study conducted in the context of the IntelliIoT project will be published as aggregate data; no personal patient data will be disclosed.

Dissemination will take place via:

1) Submission of pilot study findings for publication in international medical journals.
2) Publications in medical informatics and AI conferences and journals.
3) Presentations at congresses / meetings.
4) IntelliIoT project Work Package 6 (WP6)-specific activities.

## 2.4 Retention

Pursuant to Article 5(1)(e) of the GDPR, personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

In this context, personal data will be retained for as long as is required to fulfil the activities of the IntelliIoT Project (i.e., until the official end date of the project and the final project review demonstrators expected by the European Commission, whichever comes later) and will be permanently deleted after 10 years, based on: a) the estimated duration of the project and the time required for comprehensive data analysis; b) legal obligations / regulations.

Limitations may arise in cases anticipated by applicable law; for example, IntelliIoT may retain personal data if it is reasonably necessary to comply with any legal obligations, meet any regulatory requirements, resolve any disputes or litigation, or to prevent fraud and abuse.

In terms of implementation, data is stored in the following manner:

i) Personal Identifiable Information (PII) will be stored and encrypted in the described Patients Data Repository located at the IT department of PAGNI. Sensitive patient data will also be stored in the local data stores of the devices used by the patients enrolled in the IntelliIoT study.
ii) Pseudo-anonymized data will be stored in SharePoint and in a centralized location provided by the IT department of Philips.

The latter will allow for the analysis of the fully anonymized data to continue after the end of the IntelliIoT project, while data stored at other locations will be erased according to Section 2.5.

## 2.5 Destruction

At the end of the data life cycle, be it because the retention period (as described in Sect. 2.4 above) has expired or because one of the participants requested deletion of their data (pursuant to Article 17 of GDPR, referring to the Right to erasure), a secure deletion process will be followed.

The process will involve the use of relevant secure data erasure software to ensure that the deleted data is rendered unrecoverable, achieving full sanitization. Furthermore, an auditable report will be produced whenever this process is carried out.

# 3 DATA DE-IDENTIFICATION

As described in Section 2, all patients whose data is processed in the IntelliIoT project have provided consent for the use of the data in the project and for their participation in the study. To reduce the privacy and security risk for the patient data, we will ensure that all the data used withing the IntelliIoT environment is de-identified according to state-of-the-art procedures. In this section we provide an overview of the steps taken to safeguard the regulatory compliance and ethical conduct of the use of personal data within IntelliIoT, the de-identification approach and the corresponding tasks and tooling.

## 3.1 Regulatory compliance and ethical conduct

The regulatory compliance was reviewed by the Internal Committee Biomedical Experiments (ICBE) of Philips. The review entailed the following main steps:

1. Study Classification through the submission of a Study Request Form for the indication of risk control measures (privacy, regulatory, amongst others) that need to be put in place.
2. Dossier Completion using templates relevant for the specific study type. The templates included the following:
    a. Privacy assessment (Annex 6.1, extract).
    b. Security assessment describing the components to be developed; the logging of application execution and errors for audit and security purposes; patch management for continuous integration and development strategies, dependency management, and remote debugging; the encryption of data in transit and rest; data retention policies; and the availability and backup of data.
    c. Privacy notice (Annex 6.2).
    d. Data sharing agreement to determine the roles and responsibilities between the joint controllers University General Hospital of Heraklion (PAGNI) and the legal entity Philips Electronics Nederland B.V.
3. Approval of the Study File by a privacy coach, the Secretary of the ICBE, the assigned Reviewers, and ultimately the ICBE (ethics committee of Philips).

## 3.2 Methodology

As previously described, only de-identified data will be used within the IntelliIoT environment for development and evaluation of tools and models. Data de-identification will be carried out on site for data collected at the hospital site, and in the patient's environment for the data collected from devices, before ingestion into the IntelliIoT environment. The de-identification approach will focus both on removal of direct identifiers and on transformation of quasi-identifiers to reduce the re-identification risk. Widely adopted and validated statistical methods (e.g. [1], [2]) will be applied when needed to compute risk or re-identification, to process the data, and ensure that the re-identification risk is very low. The possible sources of data bias will be evaluated as well to identify potential bias in data and in the models developed with the data.

## 3.3 Procedure

At the time of informed consent, each patient enrolled in UC2 will be assigned to a unique project ID (code), which will be based on the sequence of enrollment (i.e., the 1st patient to be enrolled will be allocated to code 01, the 2nd to code 02, et cetera - Figure 1). A dedicated file created as a proof of correspondence between name / surname and unique project ID will be kept securely at the Clinical Trials Office of the Cardiology Department of PAGNI. All other partners involved in handling patient-derived data will only have access to the unique project ID of each patient, and not on his/her name / surname or other information that could reveal patients' identity.

Each data source used in the project has been evaluated with the support of data de-identification professionals from within the partners of the Consortium to identify direct identifiers and quasi-identifiers. All the direct identifiers will be marked for deletion.

For the quasi-identifiers, the re-identification risk for the dataset was assessed. To reach the desired low risk, data elements that create outliers were marked to be generalized (e.g., date of birth became year of birth or age). The final decision was made in order to maximize data utility while ensuring the desired low privacy risk. For the retrospective datasets collected by PAGNI, a specific privacy notice was added to the consent form that includes in full detail the data elements that are shared with the AI researchers from Philips.

The same transformations will be applied according to the defined requirements on the rest of the data to be collected. Special care will be taken with respect to data streams, to ensure that the re-identification risk remains at the selected level. During the pilot study when data will be streamed from patient devices to the hospital repository, a second privacy evaluation will be made to ensure that the process is compliant with regulations and the risk of re-identification is not increased.

## 3.4 Tools and mechanisms for ensuring privacy compliance

The pseudonymization described in Section 2.1 does not require dedicated tools (only specific mappings and generalizations implemented as tables and scripts), as instead the described privacy process and the actual pseudonymization is agreed in contract to only include removal of direct identifiers, generalization of date of birth to year of birth, and linking a pseudo-identifier to all data belonging to a single study subject. At time of patient enrollment thus, no additional tools are required beyond mapping tables and rule-based transformations. As mentioned previously, this approach ensures compliance with the privacy regulations and protects the patients' privacy rights according to the GDPR, it was reviewed by privacy, legal, security, and de-identification experts and was approved by the ethics committees of PAGNI and Philips.

In due time due to the increased volumes of data collection of patients, IntellioT will implement and validate a scalable de-identification process and pipeline that will support the efficient de-identification of all the data streams, both data collected at the clinical site and data coming from devices. We will process all the data according to the state-of-the-art methodology summarized above (which is validated and extensively used in healthcare), and the results will be evaluated by privacy and data de-identification experts.

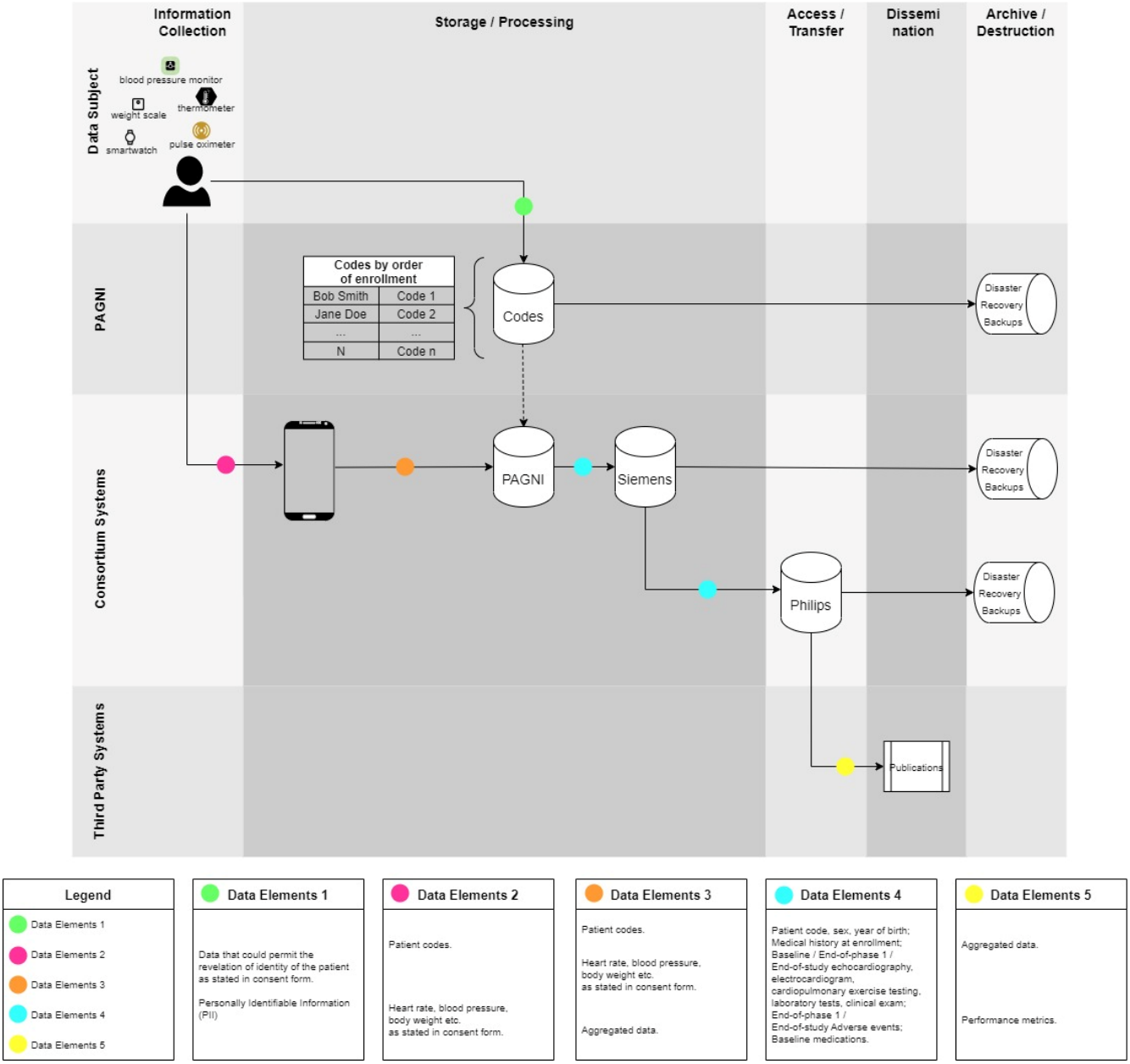


*Figure 1. The flow of data through its lifecycle as well as the collected and shared data elements.*

# 4 DATA PROTECTION

IntellIoT aims to develop a by-design trustworthy solution, encompassing security, privacy, and trust provisions across its layers and throughout its lifecycle. In that sense, IntellIoT is by inception to a large extent aligned with Article 25 of GDPR on "*Data protection by design and by default*".

Considering the scope of this deliverable, and in addition to the measures detailed in the previous subsections, pursuant to Article 32 of GDPR (referring to the *"Security of processing"*), a number of state-of-the-art technical and organizational measures will be adopted in IntellIoT to ensure that sensitive data is protected throughout its lifecycle, in all its states (in transit, at rest, in processing).

The relevant requirements and associated measures are presented in detail in Table 1.

*Table 1. Security of processing requirements and associated IntellIoT measures.*

| Requirement (pursuant to Article 32 of GDPR) | IntellIoT measures |
|---|---|
| **Pseudonymization of personal data** | See Sections 2 and 3 above for details on the pseudo anonymization and de-identification processes. |
| **Encryption of personal data** | Encryption of data at rest in the Patients Data Repository, centralized location, and local data stores.<br><br>Encryption of data in transit via industry standard Transport Layer Security (TLS [3]) protocol, end-to-end, across all sensitive communication channels. |
| **Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services** | Integration of Trustworthiness components (one of the three key pillars of the IntellIoT architecture – see deliverable D2.3) across all layers of the IntellIoT deployment. All Trustworthiness components are detailed in deliverable D4.4.<br><br>Security Assurance solution providing continuous assessment of the security and privacy posture of IntellIoT.<br><br>Integration of strong Authentication, Authorization and Accounting mechanisms, through integration of dedicated components employing standardized, industry-established technologies.<br><br>Protected, secure APIs between components.<br><br>Protected and trustworthy logging capabilities through the integration of Distributed Ledger Technologies.<br><br>Continuous monitoring of operations of assets accessing and/or processing sensitive data.<br><br>Continuous monitoring of network and involved entities through Trust-based Intrusion Detection System and Moving Target Defenses. |
| **Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident** | Continuous monitoring of availability of core services through appropriate event captors.<br><br>Engagement of Moving Target Defenses to mitigate network-based attacks.<br><br>Use of a dynamic virtual infrastructure management environment facilitating spawning of additional instances to retain availability / maintain access. |
| **Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for** | Integration of Security Assurance solution enabling the ad hoc or scheduled (periodic) assessment of the security & privacy posture of the IntellIoT deployment, also encompassing evaluation of the effectiveness of technical measures in place.<br><br>Integration of Accounting and protected logging mechanisms, with emphasis on the asset and operations involving the storage, transit, and processing of |

| | |
|---|---|
| **ensuring the security of the processing** | personal data, providing the necessary evidence for auditing and compliance assessment. |
| **In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed** | Ethics & Privacy requirements documented in deliverable D1.3.<br>Key sources of risk and threats for Healthcare Use Case documented in deliverable D2.1.<br>Inclusion of risk and impact assessment metrics within the security & privacy posture assessment of IntellIoT, as executed through the Security Assurance component, encompassing all assets (including data assets). |
| **Adherence to an approved code of conduct ... or an approved certification mechanism ... may be used as an element by which to demonstrate compliance ...** | Integration of mechanisms allowing the generation of evidence for audit and certification purposes, augmented by Distributed Ledger Technologies. |

# 5 CONCLUSION

In this deliverable we have described the primary categories of patients' data that will be collected in the context of the IntellIoT project, including: a) demographic and medical data that are routinely recorded in usual clinical practice; b) high-volume data of patients' biological parameters of interest, derived from smart devices (wearable and non-wearable). Only the physicians involved in the IntellIoT project as investigators / partners will have access to personal information that could reveal enrolled patients' identity; all other partners involved in the Healthcare Use Case of the project will only have access to de-identified data.

We have also described the methodology for de-identification and the privacy and security measures within IntellIoT as they relate to the data life cycle and data processing.

# 6 ANNEX

## 6.1 Privacy Assessment Extract

| |
|---|
| Project status:<br>(completed, to do, not applicable) |
| Which common scenarios have been considered and which one applies here?<br><br>Indicate the choice for one of the eight common scenarios |
| **A brief summary of the privacy aspects:** |

| | |
|---|---|
| **Copy information from these columns to the Clinical Studies SPCA Support document** | |
| **Categories of Personal Data** *(Select from the table below)* | |
| **'Categories of Personal Data' set out below can be chosen from the drop-down menu from when filling in the Excel table of the Clinical Studies SPCA Support document** | |
| **Data below is not collected nor received by Philips** | |
| Personal characteristics (age, gender, date of birth, place of birth, marital status, nationality) | |
| Personal characteristics<br><br>Personal characteristics<br><br>Medical information | |
| **Phase 1. Data elements below are received and processed by Philips** | |
| Medical information<br><br>Medical information | |
| **'Categories of Personal Data' set out below cannot be chosen from the drop-down menu when filling in the Excel table of the Clinical Studies SPCA Support document: please use the free text field** | |
| Results<br><br>Publications | |

| Check if applicable and addressed | What? |
|---|---|
| ☒ | 1. Dataset registration |

| | |
|---|---|
| ☐ n/a | **2. External dataset** |
| ☐ n/a | **3. De-identification team involved** |
| ☒ | **4. Information security review** |
| ☐ n/a | **5. Legal basis: Legitimate interest** |
| ☐ n/a | 6. **Legal basis: Legitimate interest & processing of sensitive data** |
| ☐ n/a | **7. Data Processing Agreement** |
| ☐ n/a | **8. Approval of the BIU privacy officer** |

## 6.2 Privacy Notice

**INFORMATION AND INFORMED CONSENT FORM**
**for participation in a clinical trial**

Dear Sir / Madam,

The purpose of the present document is to explain why we believe that you might participate in this study and what will happen if you should decide to participate. The physician who is in charge of you in this hospital is available to reply to all your questions. We ask you to read the following information carefully and then to decide freely whether you will participate in this study.

**You have no obligation to participate if you do not wish so, or if you have any hesitation relevant to your enrolment in the current study.**

**In addition, you are free to withdraw your consent for participation in the study anytime you would like to do so, without being obliged to provide a reason.**

| Short title of the investigational program you are invited to be enrolled in: |
|---|
| **Intelligent, distributed, human-centered and trustworthy Internet-of Things (IoT) environments** |
| Principal Investigator of the program |
| **Professor Georgios Kochiadakis**<br>**Head of the Cardiology Department of the University Hospital of Heraklion** |
| **Partners involved in the project:**<br>- **SIEMENS AKTIENGESELLSCHAFT (Project coordinator)**; Berlin and Munich, Germany<br>-**EURECOM**; Campus SophiaTech, 450 Route des Chappes, F-06410 Biot, France<br>-**AALBORG UNIVERSITET - AAU, Department of Electronic Systems**; Fredrik Bajers Vej 7k, DK-9220 Aalborg, Denmark<br>-**OULUN YLIOPISTO – UOULU**; Pentti Kaiteran Katu 1, FI-90014, Oulu, Finland<br>-**TTCONTROL GMBH – TTC**; Schoenbrunner Strasse 7, A-1040, WIEN, Austria<br>-**Telecommunication Systems Institute – TSI**; Technical University of Crete Campus, GR-73100, Chania, Greece<br>-**Philips Electronics Nederland B.V. (Lead of the Healthcare Usecase of the project)**; High Tech Campus 52, 5656 AG Eindhoven, The Netherlands |

EEBK03 (Έντυπο Συγκατάθεσης) 1/17

| INFORMATION AND INFORMED CONSENT FORM<br>for participation in a clinical trial |
|---|
| Short title of the investigational program you are invited to be enrolled in: |
| **Intelligent, distributed, human-centered and trustworthy Internet-of Things (IoT) environments: IntellIoT** |

**INFORMATION FOR PATIENTS AND/OR VOLUNTEERS**

**A. INTRODUCTION**

You have been diagnosed by your attending cardiologist with cardiovascular disease and you have been provided with comprehensive guidance relevant to the optimal management of your health problem. Our Department is actively involved in research in the field of your disease, aiming to contribute to broadening of medical knowledge and, ultimately, to the development of novel diagnostic and therapeutic approaches.

**B. INFORMATION ABOUT THIS STUDY**

Cardiovascular disease constitutes a leading cause of morbidity and mortality. However, despite the progress that has been achieved in diagnostic and therapeutic methods, there is still considerable margin for improvement in management strategies.

You are hereby invited to be enrolled in a clinical study that is currently being conducted in the wider context of a European program, in which the Cardiology Department of the University Hospital of Heraklion participates. This program investigates the potential use of machine learning and Internet of Things (IoT) as an adjunctive modality of clinical follow-up in patients with cardiovascular disease. Internet of things (IoT) constitutes a network between a plethora of devices and any object incorporating electronic media, software, sensors and internet connectivity, so that communication and data exchange are enabled. More simply, IoT rationale is the interconnection of all electronic devices (local network), with the potential of connection to the internet (world-wide web).

EEBK03 (Έντυπα Συγκατάθεσης) 3/17

**participation in this study, no clinical decision will be solely based on automated messages; direct instructions will be provided by your physician in any case in which a change in management will be recommended.**

Clinical findings and surrogate markers of your disease course from the period during which device-facilitated remote follow-up will be taking place, will be compared to the respective findings and markers from the control period, during which you will be followed-up as per routine practice on outpatient basis.

We inform you that the study will be conducted following the internationally defined rules of "Good Clinical Practice" and with respect of ethical principles established in Helsinki Declaration. We also inform you that this study –as well as all study-related materials or equipment, including the present Informed Consent Form- has been approved by our institution's Ethics Committee.

The management of your disease will not be influenced by your participation in the study and will comply to current standards of best clinical care (European guidelines for the management of your disease).

**Your consent only refers to the acceptance of the follow-up of simple clinical parameters with the aid of the devices that you will be given, as well as the collection and analysis of your anonymized clinical data.**

Any personal data that will be collected for the purposes of this study will be recorded anonymized in the trial's database. Any future use of clinical data and/or biological samples, if you provide your consent, will solely serve scientific / research purposes and will be performed only after approval by the competent authorities.

## C. CONFIDENTIALITY, DATA PROCESSING AND PERSONAL DATA PROTECTION

EEBK03 (Έντυπα Συγκατάθεσης) 5/17

provide your consent for participation in this study while, in parallel, opting out of receiving information about findings not related to the primary objectives of this study.

2) **Processing of your data by Philips Electronics Nederland B.V. (Lead of the Healthcare Usecase of the IntellIot project**; Address: High Tech Campus 52, 5656AG Eindhoven, the Netherlands)

a) Types of data that will be processed by Philips Electronics Nederland B.V. (Philips):

-Personal Characteristics (Subject ID, sex, year of birth)

-Medical Information (Medical history at enrolment; Baseline/End-of-phase 1/End-of-study echocardiography, ECG, cardiopulmonary exercise testing, laboratory tests, clinical exam; End-of-phase 1/End-of-study Adverse events; Baseline medications)

b) Purposes for which Philips will process your data:

To fulfil the following primary objectives and purposes:

-To extend and evaluate algorithms that can run on mobile devices and IoT (internet of things) devices, and to evaluate the use of 5G technology. With the goal to personalize recommendations and advice for instance on exercise, to the needs of individual users.

-The collected data provided in the IntellIoT project will be used for the technical evaluation of the framework and to train preliminary models.

Aggregated results of this study will be made available to the IntellIoT consortium members (https://intelliot.eu/about) and published.

.

Philips may also process your data for the following purposes:

-To ensure its medical devices and services adhere to a high standard of quality and safety;

EEBK03 (Έντυπα Συγκατάθεσης) 7/17

business or a part of a business to another company, or any reorganization, merger, joint venture, or other disposition of Philips' business, assets, or stock.

f) International transfer of your personal data:

Due to Philips' global nature, your data may be transferred to or accessed by the company's affiliates and trusted third parties from various countries around the world in order for Philips to fulfill the purposes described above. As a result, if the study takes place in a member state of the European Economic Area, Philips may transfer your data to countries located outside of the European Economic Area. Philips is required to ensure a safeguard is put in place for transfers to these countries. Some of these countries are recognized by the European Commission as providing an adequate level of protection; however, for countries that are not recognized by the European Commission as providing an adequate level of protection, Philips has put in place appropriate legal, organizational, and procedural measures to protect your data, such as:

- The Philips Privacy Rules (also known as the Binding Corporate Rules) approved by the competent data protection authorities: The Philips Privacy Rules enable the transfer of your data between Philips affiliates;
- Standard Contractual Clauses approved by the competent European Institution: These Clauses enable the transfer of your data to external third parties.

g) How long does Philips keep your data?

Philips keeps your data as long as the company needs to fulfill the purposes for which it has been collected.

The criteria used to determine retention periods include:

- How long your data is needed to perform the study.
- How long your data is needed to fulfill the purposes for which it was collected.
- Whether Philips is subject to a legal obligation to keep your data.

EEBK03 (Έντυπα Συγκατάθεσης) 9/17

1096 BC, Amsterdam, The Netherlands.

If you are not satisfied with Philips' response or believe that your data is not being processed in accordance with the law, you may contact or lodge a complaint with the competent data protection authority or seek other remedies under applicable law.

**D. POSSIBLE BENEFITS FROM YOUR PARTICIPATION IN THE PRESENT STUDY**

We believe that your voluntary participation in this study could be translated into an improved and more efficient out-of-hospital follow-up, by minimizing unnecessary healthcare visits, but this remains to be proven. However, you are certainly expected to benefit from the close clinical follow-up during your participation.

**E. POSSIBLE RISKS FROM YOUR PARTICIPATION IN THIS STUDY:**

**The design of this study does not pose any forseeable additional risk to participants, besides health risks inherent to and directly related to their underlying disease.**

**F. COST OF YOUR PARTICIPATION IN THIS STUDY:**

Your participation in this study will not come at any financial cost.

**G. YOUR CONSENT TO PARTICIPATE IN THE PRESENT STUDY:**

***We emphasize that your participation in the study is completely free and voluntary and –if you wish- you may exit the study at any time, without having to provide any explanation.***

If you do not provide your consent for participation in this study, your medical care will not be affected adversely in any way.

EEBK03 (Έντυπα Συγκατάθεσης) 11/17

**INFORMED CONSENT FORM**

**for participation in a clinical trial**

Title: **Intelligent, distributed, human-centered and trustworthy Internet-of Things (IoT) environments**

| Question | YES / NO |
|---|---|
| Did you personally sign the present form? | |
| Have you read and understood the information for patients/volunteers? | |
| Did you have the opportunity to ask any questions and discuss any issues relevant to the present study? | |
| Were you provided with satisfactory explanations / information? | |
| Have you understood that you can withdraw your consent for participation anytime you wish? | |
| Have you understood that you have no obligation to provide a reason, should you decide to withdraw your consent? | |

EEBK03 (Έντυπα Συγκατάθεσης) 13/17

STUDY PARTICIPANT NAME SIGNATURE Date:

_____ _____ _____

LEGAL REPRESENTATIVE NAME SIGNATURE Date:

_____ _____ _____

IMPARTIAL WITNESS NAME SIGNATURE* Date:

_____ _____ _____

* in case the participant or his/her legal representative(s) cannot read

INVESTIGATOR STATEMENT

I declare that I have provided the study participant with comprehensive and detailed information relevant to the character, the objectives, the procedures and the duration of this study. I also declare that I have given the participant the study information form, as well as a copy of the present signed and dated Informed Consent Form.

INVESTIGATOR
SIGNATURE_____

Date_____

EEBK03 (Έντυπο Συγκατάθεσης) 15/17

INVESTIGATOR NAME (capital letters)_____

**OPTIONAL CONSENT for being notified about incidental findings that might arise from data analysis:**

| | |
|---|---|
| **Do you consent to be notified about clinically significant incidental findings that might arise from the analysis of the data collected?** | **YES/NO** |

STUDY PARTICIPANT NAME SIGNATURE Date:

_____ _____ _____

LEGAL REPRESENTATIVE NAME SIGNATURE Date:

_____ _____ _____

IMPARTIAL WITNESS NAME SIGNATURE* Date:

_____ _____ _____

* in case the participant or his/her legal representative(s) cannot read

EEBK03 (Έντυπο Συγκατάθεσης) 16/17

INVESTIGATOR
SIGNATURE_____

Date_____

INVESTIGATOR NAME (capital letters)_____

EEBK03 (Έντυπο Συγκατάθεσης) 17/17

# 7 LIST OF ABBREVIATIONS

| Acronym | Definition |
|---|---|
| ECG | Electrocardiogram |
| GCP | Good Clinical Practice |
| GDPR | General Data Protection Regulation |
| PAGNI | University General Hospital of Heraklion |
| PII | Personal Identifiable Information |
| TLS | Transport Layer Security |

# 8 REFERENCES

[1] Internet Engineering Task Force, "The Transport Layer Security (TLS) Protocol Version 1.3", [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8446.

[2] Dankar, F.K., El Emam, K., Neisa, A. et al. "Estimating the re-identification risk of clinical data sets", *BMC Medical Informatics and Decision Making,* vol. 12, article 66, 2012.

[3] El Emam, K., Arbuckle, L., "Anonymizing Health Data", O'Reilly Media, Inc., ISBN: 9781449363079, 2013.