Privacy statement

CARRIER - “Coronary ARtery disease: Risk estimations and Interventions for prevention and EaRly detection” – a Personal Health Train project, NWO project nr. 628.011.212.

Contact

If you want to know more about the CARRIER project or how we deal with Data protection, please contact us via: *RT-carrier@maastrichtuniversity.nl*

You can also contact us at:

Maastricht University
Attn: Data Protection Officer
P.O. Box 616
6200 MD Maastricht
The Netherlands
privacy@maastrichtuniversity.nl

We will do our best to respond to your query in a reasonable amount of time.

Introduction

At the CARRIER project, the privacy of people is very important to us. That is why we have put strong measures in place to safeguard citizens’ privacy.

The CARRIER project aims to reduce the burden of coronary artery disease (CAD) by using clinical data for research. Some of the data we use have been collected specifically for this project, and with an informed consent. Other data have already been gathered for other purposes (for example, by general practitioners, hospitals, or by the Central Bureau of Statistics/CBS Netherlands). Using the data that has already been gathered is permitted under the General Data Protection Regulation (GDPR or AVG) where the new processing is compatible with the purpose for which the data have already been collected. CARRIER has gained approval from the relevant research authorities for this use of the data.

Consequently, your personal data may be processed in the project for scientific research purposes. In the following, this privacy statement will explain how CARRIER is managing and processing personal data.

What is the objective of the CARRIER project?

The CARRIER project aims to target the detection, primary, as well as secondary, prevention of CAD. CAD is the most common cardiovascular disease and one of the leading causes of death and disability. Changes in lifestyle behaviour, such as a healthy diet or physical activity can have a beneficial impact on health and help prevent the development of cardiovascular disease. Unfortunately, the current uptake of rehabilitation programs to prevent CAD is relatively low; hence, by providing a digital solution for participative self-care, the CARRIER consortium aims to reach more citizens, and to spread awareness regarding potential risk factors influencing CAD. Working in a multidisciplinary team of regional clinicians, citizens, legal experts and data scientists, the CARRIER consortium makes use of big data and artificial intelligence to build models that will drive detection and prevention of CAD. These models will help to identify patients at increased risk and will facilitate disease management. An electronic lifestyle coach will support adherence to a personalised health management plan co-created by patients and clinicians.

Due to the technology-driven nature of the research project, data protection has been paramount since the beginning of the project. Applicable international, as well as domestic legislation are considered during each phase of the project, and adhered to by the entire consortium.

Which data is being used in the project?

The CARRIER project uses citizens' personal data, in a large dataset to develop the formula and software. This data has already been gathered by our project partners, such as CBS, RNFM, MUMC+ (a full list of partners and links to their websites are provided below). In order to develop a prediction model[1] that is as accurate as possible, several types of personal data are used:

1. Special category data, such as medical or anthropometric data
2. Demographic data, such as area of residence

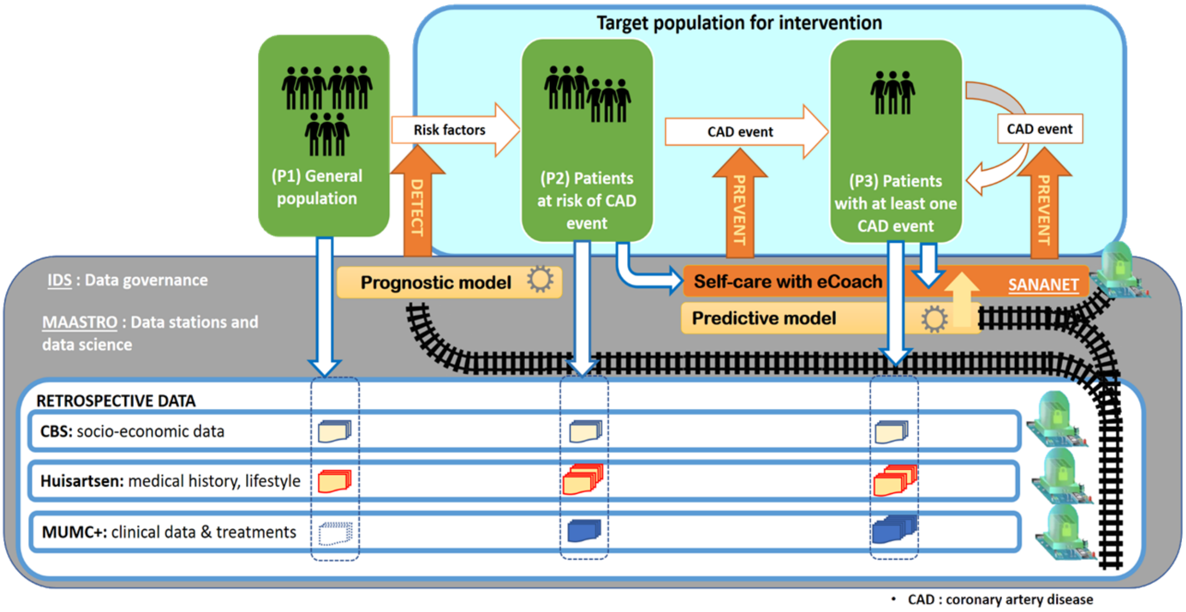
The precise list of variables included are: "*Gender, birth year, weight, height, area of residence, smoking habits, blood pressure, cholesterol, comorbidities, diagnosis of cardiovascular disease (CVD), hospitalisation for CVD, and family history of cardiovascular disease*".

How will the data be used/ processed?

Legal routes for processing/ permission

The aim of processing these various types of data is the development and validation of cardiovascular risk prediction models. These models are, in essence, a piece of computer software that contains a formula that estimates a person’s risk to develop cardiovascular disease given a set of characteristics (e.g. age, gender, medical history, or lifestyle). The CARRIER project makes use of data that has already been collected by its various partners. Since most of the data sets were gathered for research purposes, the developers of CARRIER are allowed to re-use this data, in compliance with the GDPR as well as the Personal Data Protection Act of the Netherlands.

In order to process relevant data stored within the different silos (intuitions), the CARRIER Project will make use of a specific technique known as “*Personal Health Train*” (PHT). For detailed information, please visit: https://pht.health-ri.nl/. This technique allows researchers to work with data from various resources, without infringing any privacy rights since no sensitive information will be shared. Researchers will only have access to pseudonymised data, which cannot be traced back to individuals.


Target population for intervention
(P1) General population
Risk factors
DETECT
(P2) Patients at risk of CAD event
CAD event
PREVENT
(P3) Patients with at least one CAD event
CAD event
PREVENT
IDS : Data governance
MAASTRO : Data stations and data science
Prognostic model
Self-care with eCoach
SANANET
Predictive model
RETROSPECTIVE DATA
CBS: socio-economic data
Huisartsen: medical history, lifestyle
MUMC+: clinical data & treatments
• CAD : coronary artery disease

Pseudonymisation is a process that removes the information that directly identifies an individual (e.g. name, address) from the dataset, and replaces them with a code. We need to be able to use coded data so we can link data kept about individuals in different datasets. This is not so the particular person is identifiable, but so that the characteristics relating to the individual can be connected together between the datasets. Hence, the names of the people to whom the code relate is not available to the researchers.

How do we protect the data?

Privacy and data protection are considered in any design and development step throughout the entire project. To elaborate, CARRIER uses IT security measures to protect for unwanted access or corruption of the data. All involved parties (UM, CBS, MUMC+ and Zuyderland) have standard operating procedures in place to guarantee a high level of security. The IT infrastructure set up for CARRIER will be tested with a penetration test before data is placed in it.

Furthermore, privacy-preserving techniques (i.e. secret sharing[2], homomorphic encryption[3] and synthetic data[4]) are applied to prevent each institution's data being revealed to other parties within the project. Last, CARRIER will ensure that it is not possible to reproduce individual level data from the developed models.

What should I know as potential data subject?

The data will be stored in secure IT servers throughout the duration of the project and for four years after the publication of the results of our study. We need to keep the data for that extra four years for reproducibility purposes, so that we can show the robustness of the science we have developed.

If you are now reading about the project and start wondering if your data might be included in the CARRIER research, please do not hesitate and contact us for further information via:
RT-carrier@maastrichtuniversity.nl
Below is a brief list summarizing your rights as potential data subject:

- You have the right to access your data and to receive details on the personal information CARRIER is using from you
- You have the right to receive information on what is done with your data
- You have the right to change or adjust your data in case of incorrect or missing information
- You have the right to object to the processing of your personal data
- You have the right to be 'forgotten' (to have your personal data erased)
- You have the right to opt-out and to restrict the processing of your personal data by CARRIER

Due to the use of the PHT, CARRIER will only be able to provide you with parts of the information or services you require. To be able to exercise all you rights as potential data subject, please find below a detailed list of further contacts:

- If you are a patient at Maastricht UMC+, you can exercise your data rights here: https://www.mumc.nl/patient-bezoeker/praktisch/rechten-en-plichten/uw-medische-gegevens

- If you are a patient at Zuyderland MC, you can exercise your data rights here: https://www.zuyderland.nl/ziekenhuis/patientinformatie/klantcontactcentrum/aanvraag-inzien-eigen-medische-gegevens/

- If you think your data might be included in the RNFM Maastricht dataset, you can exercise your data rights here: https://www.huisartsgeneeskundemaastricht.nl/algemene-privacyverklaring-um/

In order to prevent the abuse of those rights or any misconduct, our partners may ask you to identify yourself.

In case of questions, complains or comments

If you have any questions, complains or comments about this privacy statement or about the Data management infrastructure at Maastricht University, please contact:

Maastricht University Data Protection Officer PO Box 616 6200 MD Maastricht
privacy@maastrichtuniversity.nl
You can also contact UM's data protection officer directly via fg@maastrichtuniversity.nl.

Finally yet importantly, we would like to inform you that you have the right to complain to the Dutch Data Protection Authority. Details of how to do this can be found on the Data Protection Authority's website (www.autoriteitpersoonsgegevens.nl).

Glossary:

- [1] **Model** – mathematical formula that can be adjusted using data
- [2] **Secret sharing** – technique by which a secret number is split into two or more components so that calculations can be made without revealing the original number
- [3]**Homomorphic encryption** – encryption technique by which numbers are transformed to be illegible but in a way that can be added or multiplied together and then decrypted once added / multiplied.
- [4] **Synthetic data** – made up data generated by a model based on patterns learnt from real data