PRIVACY IN DIGITAL HEALTH A POSITIVE DRIVER FOR INNOVATION

TNO Whitepaper

Marc van Lieshout
Wessel Kraaij
Hanneke Molema

CONTENTS

INTRODUCTION

MANY PEOPLE TODAY USE WEARABLE DEVICES AND DO-IT-YOURSELF (DIY) TESTS TO MONITOR THEIR HEALTH. WHILE DOING SO, THEY GENERATE MASSIVE AMOUNTS OF PERSONAL DATA, SUCH AS DATA ABOUT DAILY ACTIVITIES, HEART RATE, BLOOD PARAMETERS AND SLEEP.

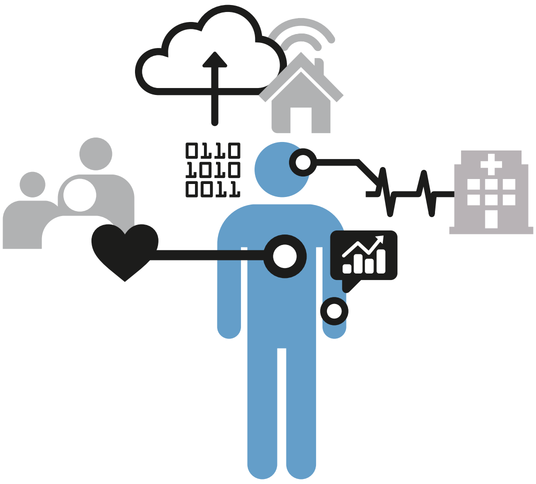
RESEARCH SHOWS THAT MANY PEOPLE ARE WILLING TO SHARE THEIR DATA WITH HEALTHCARE PROVIDERS AND EVEN APP PROVIDERS WHEN IT HELPS IMPROVING THEIR HEALTH CONDITION. THIS IS IMPORTANT, BECAUSE THESE DATA ARE A RELEVANT FACTOR FOR INNOVATIONS WITHIN HEALTHCARE.

Personal health data are however sensitive data; they reveal aspects of a person's health condition, of health-related behaviour, of family members, of situational factors that people are reluctant to make public or to share.

TNO considers responsible processing of these data and other adequate safeguards for privacy a highly relevant precondition to achieve successful innovations in digital health(care). To develop solutions hereto, TNO integrates a diverse set of disciplines and background knowledge in a number of challenging propositions for digital health and privacy. These propositions address challenges of both public and private stakeholders in healthcare. And they place the client in the focal point of the care process.

TNO aims for an orchestrating and leading role in how innovation and privacy can be reconciled in a positive and assuring manner for healthcare. This positive perspective on the role of privacy in healthcare is crucial and combines well with emerging trends, such as the on-going development of personal portals that follow agreed standards (MedMij). Or the need for a sophisticated research infrastructure that enables the use of personal data for research purposes (Health-RI).

In this white paper we elaborate on TNO's positive view on how to capture the opportunities for improving healthcare with personal health data while safeguarding the privacy of clients. We explain how our supportive concept for privacy can offer organisations the best of both worlds. We present our roadmap for future development of privacy respecting digital health and invite partners to join us in realising these ambitions.

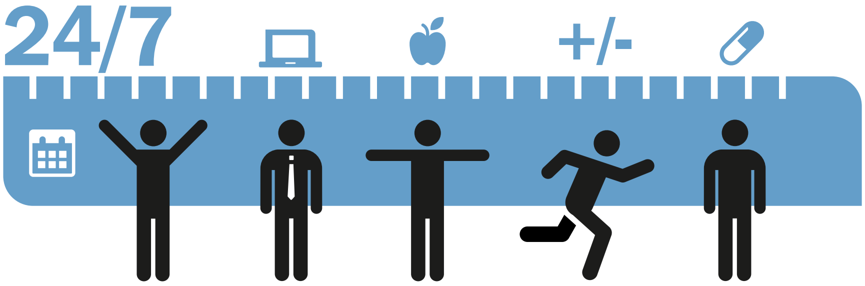


PRIVACY: FROM DEFENSIVE TO POSITIVE CONCEPT

PRIVACY IS CONSIDERED A HUMAN RIGHT TO BE SAFEGUARDED. THE CHARTER FOR FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION COMPLEMENTS PRIVACY AS FUNDAMENTAL RIGHT (ARTICLE 7) WITH A SEPARATE RIGHT TO THE PROTECTION OF PERSONAL DATA CONCERNING A PERSON (ARTICLE 8). IN ADDITION, THE INTEGRITY OF THE BODY HAS ALWAYS BEEN A RELEVANT RIGHT.

Organisations fear that these rights will hamper innovation, leading to reluctance to engage with activities that might infringe upon these rights. But this is not the position TNO adopts.

TNO considers the right to privacy and the right to the protection of persons with regard to the processing of their data as an incentive to innovate. These rights enforce organisations to enhance internal and external transparency on how they deal with the data they process. They improve clarity on roles and responsibilities, on what data processes an organisation is engaged with, for what purposes, by whom. They also enable organisations to demonstrate how the data are collected, processed, secured, stored, disseminated, etc., for what purposes, under what conditions, to whom, and what rights individuals can exercise.



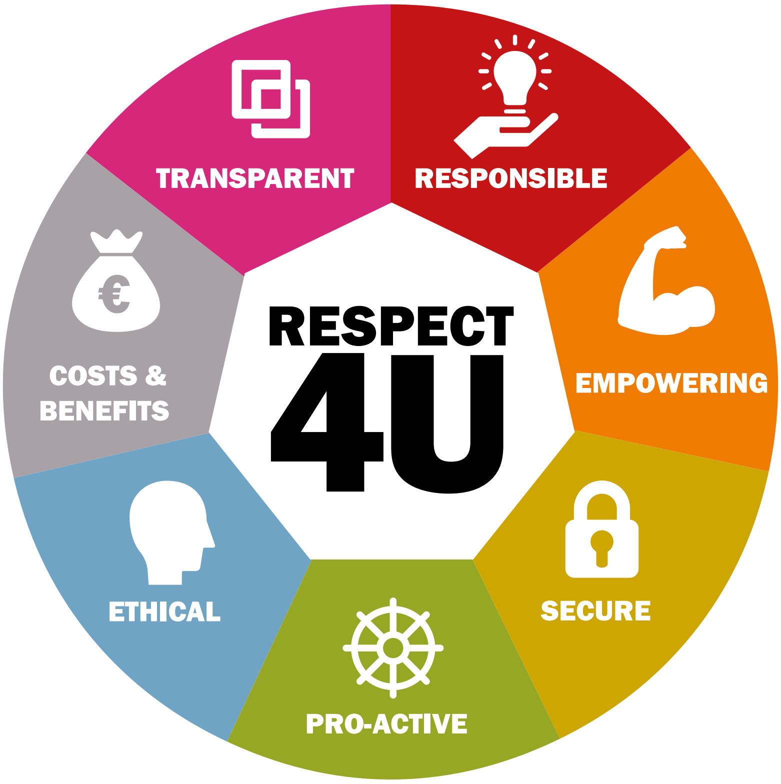
MEDMIJ
NICTIZ, the Patients Federation Netherlands and the Ministry of Health, Well-being and Sports have joined forces to create a trusted framework that shows which requirements personal healthcare portals should fulfil to offer the proper tooling and experience to clients. This framework is called MedMij. MedMij offers Rules of Engagement that support data exchange activities covering all foreseeable situations between patients and healthcare providers in primary care, secondary care and tertiary care as well as data exchange with quality assurance institutes and for academic health research. The framework is under development. MedMij takes the general data protection rules (GDPR) obligations into consideration.
See https://www.medmij.nl/ for further information.

To meet the challenges that processing of - sensitive - personal data introduces, TNO has developed a privacy framework called RESPECT4U. RESPECT4U principles propose organisations to make the turn from privacy as defensive concept to a positive one. The principles are based on relevant regulations concerning the protection of persons with respect to the processing of their data. It empowers individuals, helping them to exercise control over their data and thus enhancing their autonomy. RESPECT4U helps meeting other regulatory obligations, such as the obligation to offer clients the opportunity to indicate which care professionals are entitled access to their data. RESPECT4U is leading for TNO's vision on how digital health innovations can be promoted while safeguarding privacy to individuals. It reinforces the opportunities to realise privacy respecting solutions that contribute to improving health and well-being.

RESPECT4U: TNO'S APPROACH

THE RESPECT4U PRINCIPLES COVER SEVEN OVERARCHING ISSUES HEALTHCARE ORGANISATIONS SHOULD TAKE INTO ACCOUNT WHEN PROCESSING PERSONAL DATA : **R**ESPONSIBLE, **E**MPOWERING, **S**ECURE, PRO-ACTIVE, **E**THICAL, **C**OST AWARE AND **T**RANSPARENT.

These principles lead to a well-thought mix of organisational and technological measures. They cover different fields of actions such as promoting innovative healthcare solutions by outlining privacy risks and identifying mitigating measures. They promote trust and empowering clients through offering tools for transparency and empowerment. They emphasize secure data processing as a relevant principle that feeds into measures based upon privacy by design and by default. And the demonstration of accountability is a principle that is encompassing for all data processing activities. We concisely present the seven principles.



- Key to the approach is the overall goal to be realised: a **responsible processing of personal data**. This can be demonstrated by adherence to a Code of Conduct, adoption of certification schemes and seals, adherence to privacy standards, clear demonstration of accountability measures, and demonstration of internal learning strategies such as scoring the privacy maturity of an organisation.

- The second principle focuses on **empowering the persons whose data are processed**. By informing these persons on data that are collected, processed, disseminated etc., by offering them the possibility to exercise control over the processing – for instance by enabling them to indicate whether they are willing to participate to trials – individuals will become engaged, trust will be enhanced, and efficiency of processes will improve, for instance because inaccurate data are corrected more swiftly. Privacy dashboard are an instrument in achieving this.

- For **secure handling of personal data** innovative solutions are under development and already available. Trusttester is an instrument developed by TNO that helps securing identification and authorisation procedures. Within healthcare, TNO is developing advanced homomorphic encryption schemes that support secure processing of personal data.

- The bottom-line of the fourth principle is that it is better to be safe than to be sorry: **pro-actively inventorying risks and designing systems with an eye to privacy**. Data protection impact assessments are obliged when dealing with special categories of data, such as health data. Privacy by design and privacy by default imply that privacy requirements are included in the initial phases of systems design and that privacy remains a relevant feature throughout the life cycle of a system. Privacy design strategies and patterns help structuring and systematising what is needed to be done. The COMMIT-SWELL project, coordinated by TNO, researched these patterns.

- Some risks are however hard to discern yet. Especially with the rise of machine learning techniques, the ethical principle of **fairness and just treatment** becomes more prominent. Not only can decisions, made by automated systems, lead to unfair treatment, stigmatisation, exclusion and discrimination. But also it is sometimes difficult if not impossible to explain the logic of decisions reached given the way these algorithms function and the complex manner in which data are used in these algorithms. Within healthcare, research increasingly focuses on detecting correlations out of a large heap of structured and unstructured data. This may also infer ethical problems, for instance when it comes to explaining why someone will receive a specific treatment while someone else with seemingly similar symptoms is excluded from the treatment. TNO has realised an Early Research Programme, called Explainable AI, to study these challenges.

- The sixth principle focuses on **balancing costs and benefits**. Costs of having to adapt systems in order to meet legal obligations can discourage organisations to do the necessary investments when benefits are not clear. Sometimes costs have to be made directly, and are in hard currency, while benefits are long term and less straight forward. Benefits can be made concrete as well, for instance in the improvement of health for clients who are willing to share their data being assured that these data are processed responsibly. Other benefits relate to preventing data breaches to occur, preventing fines because of faulty procedures or denial of rights and increased efficiency because of improved streamlining of roles and responsibilities. Within TNO, a specific department constructs sophisticated cost-benefit analyses and business models that can be tuned towards privacy issues.

- The last but certainly not the least principle is the obligation to offer **transparency on data processing activities**. This is the counterpart of empowerment. Transparency is a legal obligation: for what purposes, on what legitimate ground are data processed, what technical and organisational security measures are taken, how are rights granted and enabled, etc. Within RESPECT4U, transparency also relates to organisational transparency: awareness of roles and responsibilities, awareness of goals and objectives. A transparency dashboard can be presented as the counterpart to the privacy dashboard (see Empowerment).

4U

"RESPECT FOR YOU AS A PERSON IN A TIME OF INCREASINGLY DIGITALIZED INTERACTIONS AND INNOVATION" is the central message TNO wants to convey in the acronym RESPECT4U. But it is not only the single individual is at stake. With the addition '4U' TNO wants to express the relevance of a responsible approach towards using personal data for:

- 1U: the individual;
- 2U: relations between individuals;
- 3U: relations within groups ('Three is a crowd');
- 4U: the group of groups, society at large.

RESPECT4U thus not only focuses on principles related to rights and obligations referring to the individual but considers privacy to be a relevant feature of society at large.

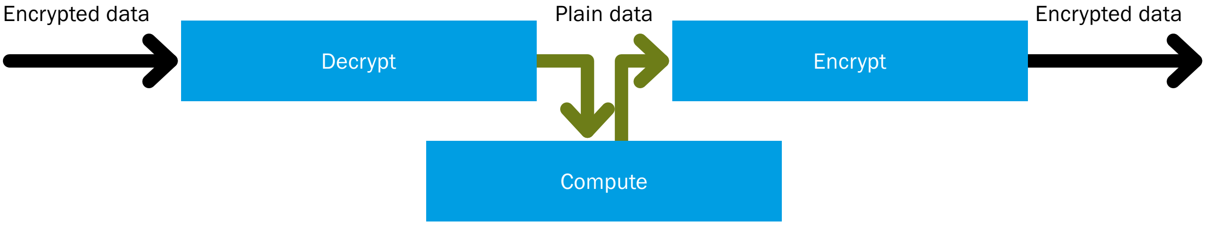
PRIVACY AS BUSINESS PROPOSITION

TNO HAS CREATED A NUMBER OF BUSINESS PROPOSITIONS THAT TRANSFORM THE PRINCIPLES INTO RELEVANT AND CHALLENGING RESEARCH AND INNOVATION ACTIONS. TNO INVITES ITS PARTNERS TO COOPERATE IN THE ELABORATION OF EACH OF THESE PROPOSITIONS. THE PROPOSITIONS REFER TO TECHNICAL, ORGANISATIONAL, ETHICAL AND SOCIETAL CHALLENGES. EACH OF THESE CHALLENGES HELPS REALISING ONE OR A NUMBER OF THE RESPECT4U PRINCIPLES

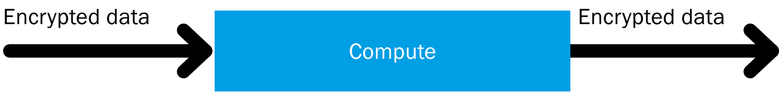
PROCESSING SECURED DATA – PRINCIPLE OF SECURITY

Advanced cryptographic techniques enable processing encrypted data without the need to decrypt them. This allows for specific analyses, such as identifying specific classes and grouping specific patients together without revealing identity information. Herewith, these techniques also allow integration of data from different sources and sharing data analyses with others, without sharing the (sensitive) meaning of the underlying data. TNO performs fundamental research in which advanced cryptographic techniques (algorithms) are developed in order to analyse data of patient groups without revealing specific patient related data. TNO participates to the EU H2020 project BigMedilyctics. The objective of this project is to improve the treatment of heart failure by combining clinical information about patients with health insurance claims data. Risk models are developed using the encrypted data sources without actually disclosing the data to the researchers.

Traditional encryption



Homomorphic encryption



PRIVACY DASHBOARD FOR HEALTHCARE – PRINCIPLE OF EMPOWERMENT

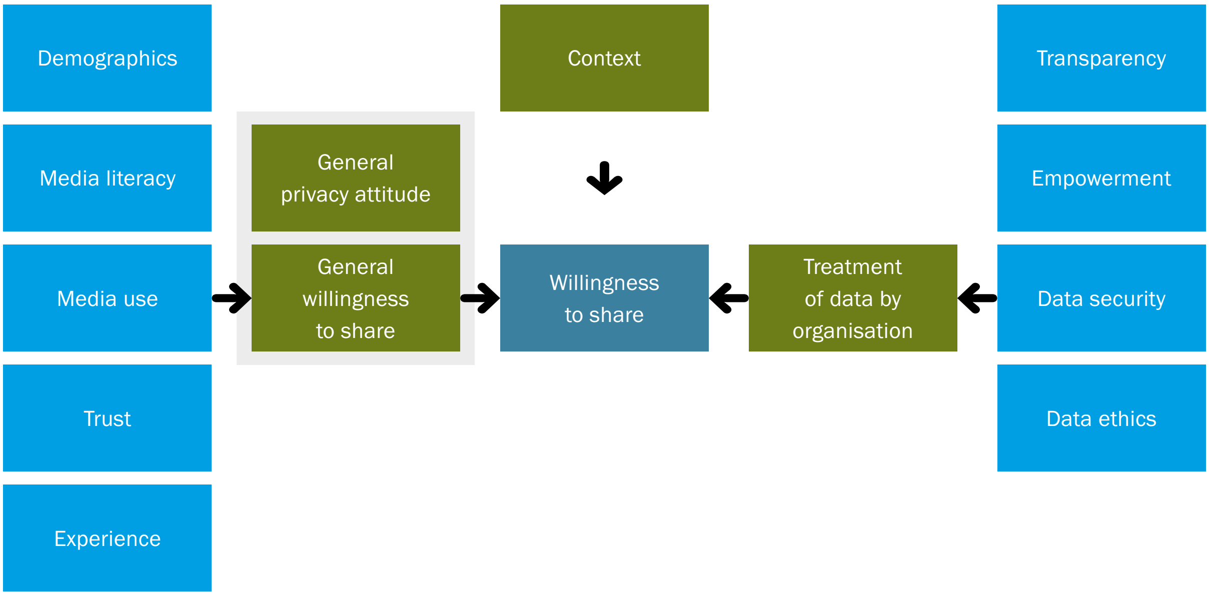
In healthcare settings various developments occur at the same time, each with their own impact on a responsible processing of personal data. One such example is the obligation to integrate extra-mural midwives care with hospital-based midwives, gynaecological care and with extra-mural maternity care. Most relevant driver for this integration is the integral funding of pregnancy-related care. In close cooperation with “IGO Geboortehart”, a health cooperation in formation in the province of North Holland, TNO developed a prototype of a privacy dashboard that eventually will enable pregnant women to be informed about and keep control over their data. The design of the dashboard was based on a survey in which the willingness to share data was inventoried against the privacy preferences of pregnant women. The perspectives of the various caregivers were included as well. The prototype of the dashboard was tested in focus groups and improved where feasible. The dashboard is ready for expansion and testing in follow up projects. TNO invites partners to join these projects.

BUSINESS MODEL FOR PRIVACY IN HEALTHCARE – PRINCIPLE OF COSTS AND BENEFITS

TNO uses a variety of models to investigate the various elements of a business proposition of privacy in healthcare. Next to advanced Cost-benefit analyses that include societal implications, business impact assessments are under development to assess and value various sorts of costs and benefits when it comes to privacy in digital healthcare. Costs are of various kinds, covering material and immaterial costs, immediate and long term costs. Benefits are explored likewise. TNO explores the possibility to finetune existing methods towards privacy-issues. It invites stakeholders to exploring how these methods can be made applicable to healthcare situations.

WILLINGNESS TO SHARE – PRINCIPLE OF EMPOWERMENT

Usually, privacy is considered to be a value in itself. TNO has developed a model, based on socio-demographic features, psychological determinants and systems characteristics in which privacy is related to the conditions that need to be fulfilled so that people are willing to share their data. The model enables a proper understanding of how individuals appreciate their privacy, how they experience the safeguards offered and how they include the context in deciding whether making their data available for specific purposes. Organisations can use this to tune their approach towards their data processes such that it optimally meets clients’ needs and expectations. The model has already been explored in healthcare settings. The initial results show the model to be promising for acquiring advanced insight in influential personal factors concerning attitude, preferences and socio-demographic components that determine the willingness of patients to share data. TNO is eager to cooperate in researching patients attitudes and exploring the lessons to be learned for including these perspectives in systems design. On top of the results of investigating the willingness to share, TNO will explore how this can be embedded in so-called health data cooperatives, approaches in which patients control their data in a cooperative manner.



Factors that play a role in a willingness to share

PRIVACY IN DIGITAL HEALTHCARE: THE WAY FORWARD

THIS WHITEPAPER INFORMS ABOUT TNO'S PROPOSITION WITH RESPECT TO THE RESPONSIBLE PROCESSING OF PERSONAL HEALTH RELATED DATA. THIS PROPOSITION ANSWERS TO THE INCREASING NEED FOR SOPHISTICATED APPROACHES THAT HELP RECONCILE THE NEED FOR PRIVACY WITH THE OPPORTUNITIES HEALTH DATA OFFER FOR IMPROVED HEALTHCARE.

LEGAL OBLIGATIONS

Three legal frames determine what constraints need to be fulfilled when processing health related data. First, medical treatment requires informed consent, and the medical professionals are bound to professional secrecy concerning the client and the treatment. Second, from 25 May 2018 onwards, the General Data Protection Regulation will enter into force. This regulation determines what rights data subjects have, what obligations controllers and processors have and what general conditions need to be fulfilled. Health data are a special category of data that require additional safeguards. Health related research, on the other hand, is considered to serve a public interest and enjoys specific exemptions. The third legal frame is the recently adopted Act on client rights in care. This Dutch act obliges healthcare providers to grant relatively fine-grained consent rights to clients (being able to determine which category of care givers is given access to their data).

We see many organisations struggle with finding the proper balance. Our privacy principles, encapsulated in the acronym RESPECT4U, offer these organizations the starting point on challenges to be addressed, the guidelines to understand what are basic requirements for each of the perspectives and the instruments to be exploited. In this paper, we address the way forward for privacy in digital healthcare in a number of research & development perspectives that form the kernel of TNO’s privacy proposition in health care. TNO invites stakeholders to cooperate in both exploring the fundamental research issues and in developing appropriate tooling and knowledge for the application oriented challenges.

PI.LAB

TNO has joined forces with Radboud University and Tilburg University and has established the Privacy and Identity lab (PI.lab; www.pilab.nl). This enables the combination of technical, organisational, legal, strategic and user-oriented expertise. Dedicated technical solutions – such as the PEP-project at Radboud Medical centre, focusing on patients with Parkinson’s disease (http://pep.cs.ru.nl/) and PRANA Data in which TNO and Radboud collaborate in order to develop novel cryptographic approaches to processing data (https://www.pranadata.nl/) – are developed to innovate healthcare processes with an eye to privacy.

Marc van Lieshout
Wessel Kraaij
Hanneke Molema

Contact
Marc van Lieshout
STRATEGIE EN BELEID
📍 Locatie Den Haag – New Babylon
✉ marc.vanlieshout@tno.nl
☎ 088 86 67 125

TNO innovation for life

TNO.NL