data security and privacy, digital healthcare, smart health, patient privacy, user-centered design, healthcare, semantics

Smart Health

Privacy as a Service: Protecting the Individual in Healthcare Data Processing

Xiang Su, Jarkko Hyysalo, Mika Rautiainen, Jukka Riekki, and Jaakko Sauvola, University of Oulu

Altti Ilari Maarala, Aalto University

Harri Hirvonsalo and Pingjiang Li, University of Oulu

Harri Honko, Tampere University of Technology

Health applications involve many data sources, individuals, and services that work against guarantees that an individual's personal data will not be used without consent. The proposed privacy-centered architecture integrates data security and semantic descriptions into a trust-query framework, enabling the provision of user consent as a service.

Healthcare's transition to the digital world has already reaped benefits such as more efficient processes and cost savings and has paved the way for new services and business models. However, the myriad organizations providing and consuming data sources and services have given rise to challenges, particularly with regard to how users can be assured that personal data is used only with their consent.

Recognizing privacy as a key obstacle to the full promise of digital healthcare, in 2012, the European Commission drafted the General Data Protection Regulation (GDPR), which became regulatory directive for the EU in May 2015. EU member nations must incorporate the directive in their laws by May 2018. The GDPR recognizes that individuals need to control their own data, but it also states the need for trust to be built into personal data services through a combination of transparency, interchangeability, public governance, respectable companies, public awareness, and secure technology. Control is realized through consent that determines what data services can fetch and how it can be processed. Thus, the regulation has a twofold objective: restore control to individuals over the use of their personal data and simplify the regulatory environment for business services. Specifically, the regulation calls for provisions to ensure user consent and to coordinate data services. According to the GDPR, "user consent" is an explicit indication of the data subject's wishes and "signifies agreement to the processing of the subject's personal data, either by statement or by clear affirmative action."[1]

To support this reform, we developed a privacy-driven architecture that provides tools for providing user consent as a service within the MyData infrastructure.[2] MyData is a procedural framework for describing personal data management that considers both the individual's digital rights and the healthcare organization's needs. It essentially acts as a bridge between multiorganizational data silos and fully decentralized Web-based systems. Our architecture works within the MyData approach to incorporate privacy as a service (PRIAAS), which facilitates the management and reuse of private health information. PRIAAS is designed to accommodate a large number of data sources, individuals, and services—even when they are not known to the user. The architecture integrates data security and semantic descriptions into a trust-query framework to provide the interoperability and cooperation that health services will increasingly require. PRIAAS's benefits include safer data management, cost and process savings, and the ability to handle the multiprovider services that are often inherent in newer business models.

The sidebar "Guiding Architectural Principles" describes five principles that we followed in compliance with the GDPR and the MyData approach. PRIAAS is the first open solution that conforms to the GDPR, is poised for widespread use in Finland (an EU country), and is endorsed as part of the Finnish government's spearhead agenda.

Consent Standards

Although personal information—whether a name, photograph, email address, bank details, or medical information--is routinely shared digitally across national borders, mechanisms remain organized around national boundaries, specific service provider rules, and legal frameworks.[3] Consent is typically through hardcopy signatures or static online interactions, such as filling out forms or clicking buttons and opt-in checkboxes. These static, actor-driven mechanisms are obviously ill suited to scaling and interoperability, and most fail to comply with requirements for distributed health services.

The GDPR was motivated in part by the need to move consent further into the digital realm, and other standards also address these limitations—notably the User Managed Access (UMA) protocol[4] and the Minimum Viable Consent Record (MVCR) specification.[5] Like GDPR, UMA and MVCR aim to give individuals unified control points for authorizing who and what can get access to their digital data, content, and services. All three are founded on simplicity, ease of use, user-centeredness, transparency, and standardization. GDPR sets the legal framework that calls for explicit, unambiguous and informed consent, transparency, and interoperability, whereas UMA and MVCR provide authorization and consent technologies that address GDPR-based requirements.

User Managed Access

UMA is an access-management protocol that gives individuals control over their personal data, content, and services. The protocol, which is based on the OAuth 2.0 standard, focuses on connecting a service that provides an individual's personal data to another service that consumes the same data in a way that allows the individual to

securely manage data access.

PRIAAS adopts several UMA protocol characteristics, including

- unified access control under a dedicated online service;
- application of the same policies across multiple sites;
- support for claims-based access policies, such as “over 18;” and
- access control that is easy for the individual to manage.

Minimum Viable Consent Record

MVCR describes requirements for creating a legitimate digital consent record, known as a consent receipt, aiming to minimize the information that individuals need to address to enable their explicit consent. The consent receipt serves as the individual’s basis for communicating to organizations about consent details and how the receipt can be used to authorize data access. We adopted MVCR as part of our consent record because it is the best available solution for describing consent in a universal machine-readable record.

Human-Centric Design Requirements

As the EU model shifts to enable more flexible exchange of healthcare data yet keeps exchange control in the hands of individuals, so system architecture must shift to human-centric designs that are built around regulations such as the GDPR.

Figure 1 illustrates how the human-centric paradigm translates into an architectural design. To ensure trusted and fair use of data across organizations, the GDPR imposes user rights that force organizations to build tools enabling informed user consent for data management, delivery, and exchange. In Figure 1, the roman numerals represent these eight user rights:

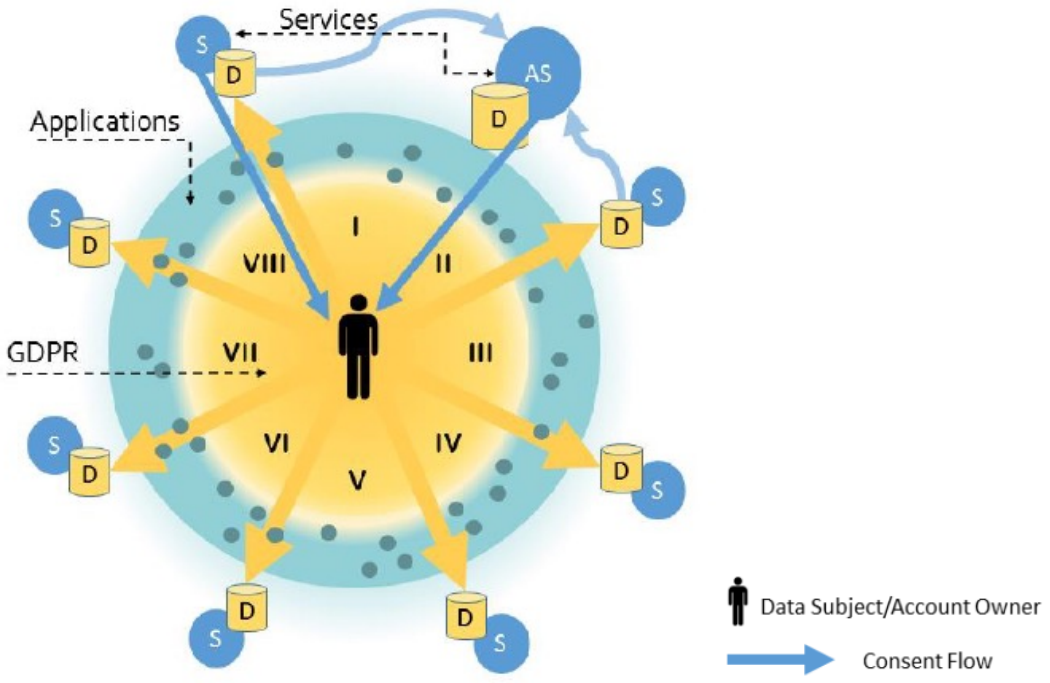


Figure 1. Aspects of a human-centric health services architecture. The individual produces data (D), which services (S) are designed to collect through a process imposed by an organizational entity. Applications (blue ring) present interfaces to users, who are increasingly involved in the organizational process of collecting and using their data. Aggregator services (AS) access different data repositories to add new value by correlating and analyzing data from a variety of organizational sources. The roman numerals in the yellow section represent enabling rights as set forth in the European General Data Protection Regulation (GDPR).

I. the right to unambiguous consent;
II. the right that only relevant, necessary, accurate, and legitimate data is processed in a specific, fair, and transparent manner;
III. the right to access one's own personal data;
IV. the right to be properly informed when personal data is processed;
V. the right to rectification;
(VI) the right to protection against the use of personal data for automated profiling;
(VII) the right to be forgotten; and
(VIII) the right to security measures.

Roles and Responsibilities

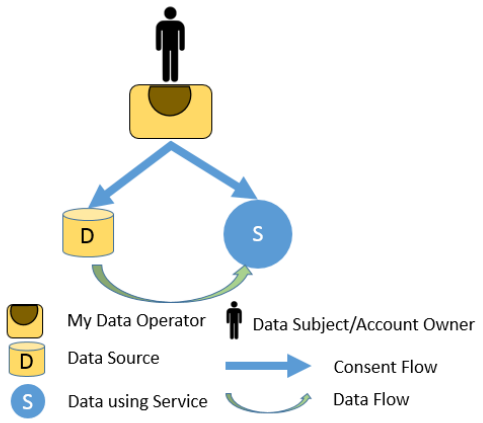
One of the central ideas in GDPR is that the control resides with the individual, who must be made aware of how personal data will be used before granting consent for its use. This requires centralized consent management in a distributed environment. For PRIAAS, this consent management is built on the MyData approach, which provides

tools for tasks such as creating a service contract that honors rules for data exchange.

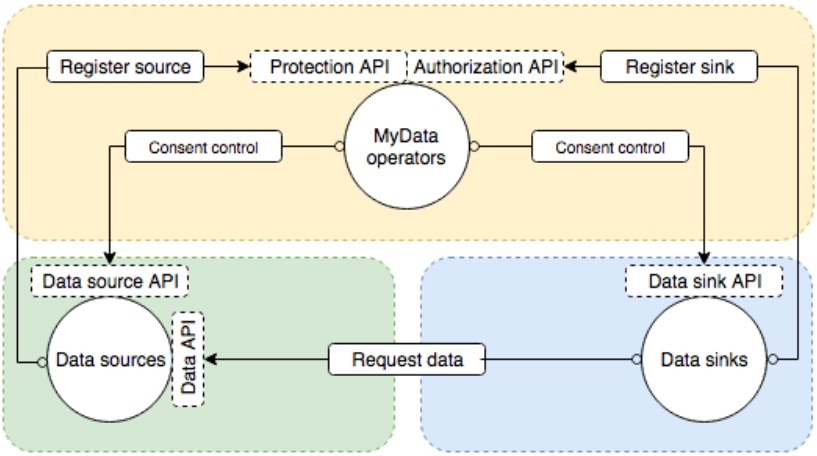
Managing consent

Central to the MyData approach is the MyData operator, a GDPR-compliant entity for service registration and consent management. Individuals use the operator to arrange and manage data exchange between sources and sinks, which are the entities that store, represent, and process data for user applications. MyData emphasizes portability and minimizes service provider lock-in, so individuals can choose MyData operators and migrate them. This account portability tends to increase trustworthiness because users have more control over processing.

As Figure 2a shows, the MyData operator manages consent through an individual's MyData account but the data itself is not necessarily streamed through the server hosting this account. The account maintains information on how the individual's personal data is connected to different services and the legal permissions and consent sources for data use. Figure 2b shows a more detailed representation. Data sources and services consuming data exchange information with the MyData account use MyData compliant APIs. Individuals can grant access and give or cancel permissions for multiple



data sources and services using this centralized interface. Any service provider can build a MyData API and enable their service to be connected with MyData accounts. Individuals can have multiple MyData operators and switch them as needed.



(a)
(b)

Figure 2. Consent management through MyData with our privacy-as-a-service (PRIAAS) system. (a) The MyData operator manages consent flow between the data source APIs (D) and the services consuming that data (S). (b) A more detailed diagram shows roles, interactions, and liabilities. In (b), the yellow screen represents the data owner. The MyData operators control consent and have protection and authorization APIs to both data sources and services consuming that data (data sinks), the green and blue screens represent data sources and their APIs and data sinks and their APIs.

Consent management through MyData operators is a novel concept that lets users arrange and manage data exchange between sources and sinks. Through their MyData account, individuals can view, manage, and control consent easily and transparently through one operator's user interface. The resulting authorization process is simpler than UMA-based authorization, which requires multiple interactions to enable authorized data transfer from source to sink..

User accounts held and managed by one or more trusted MyData operators also provide individuals with logical paths for controlling their personal data in complex environments of numerous data sources and consumers. Organizations acting on behalf of individuals can set up these accounts, or individuals can setup their own account services and provide them to organizations.

MyData operators provide Web APIs that register sources and sinks through protection and authorization APIs. Services that implement the roles of sources and sinks must provide APIs for exchanging consent information, with the MyData operator acting as a broker. In practice, sources can use these APIs to inquire about the sinks' trustworthiness level before providing data access. Actual data exchange happens between sources and sinks without involving the MyData operator, which keeps the data architecture flexible and the MyData operator's role lightweight. Consequently, a variety of organizations can establish and maintain an operator service—which is important in accelerating the widespread adoption of a MyData ecosystem.

Creating a service contract

Figure 3 is a high-level sequence diagram of the process for creating a service contract, managing consent, and transferring data. As (a) denotes in the figure, the process begins when users connect at least two services (source or sink) to their MyData account. Only connected services can receive consent.

In the second main step, (b), a sink is chosen, the user interface lists compatible sources and vice versa. The individual authorizes a sink to fetch data from a source and use this data according to rules that the user defines. The MyData operator records the parties involved in data use, the data being shared, and the rules for using in a pair of consent receipts that are stored in the user's MyData account and delivered to the sink and source. The operator constructs and cryptographically signs a token, which the sink

uses to prove its authorization to the data specified in the consent receipt.

In the third step, (c), the sink makes a data request to the source presenting the token. Finally, the token and request description are delivered to the MyData operator, which uses previously stored information to determine whether the sink is authorized to access the requested data.

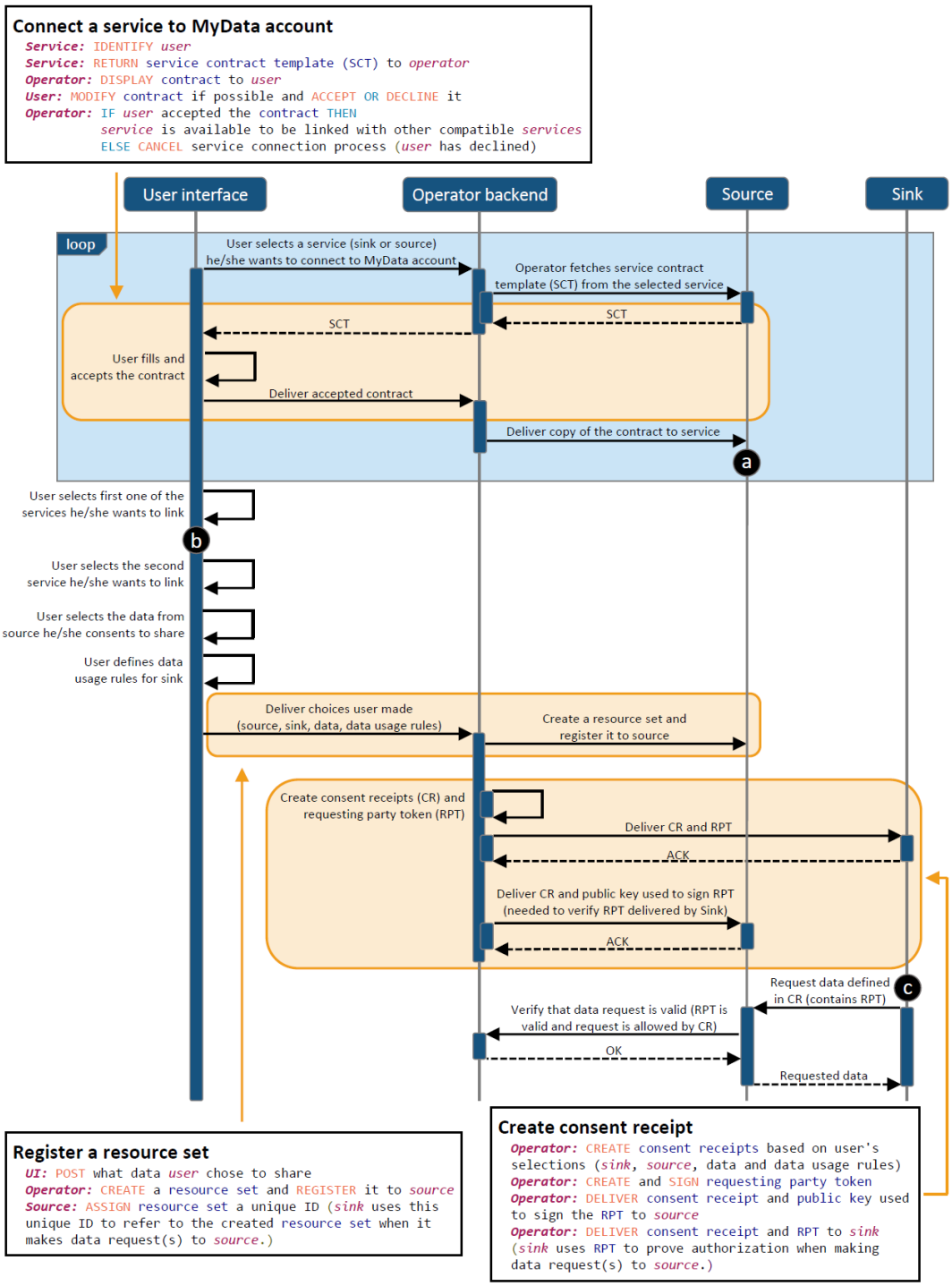


Figure. 3. High-level sequence diagram of consent creation with examples from our sample implementation with multiple providers. (a) The user connects at least two services to his or her MyData account. Connected services are authorized to hold or release data. (b) If the first service selected is a sink, the user interface lists compatible sources; if it is a source, the interface lists compatible sinks. (c) Once consent is given, a sink can request data from a source.

Benefits of PRIAAS and MyData

PRIAAS and MyData provide an open architecture with compelling benefits, such as ease of service expansion, flexible privacy monitoring, more efficient authorization relative to UMA, conformance with emerging regulations, cost savings, and improved health.

Ease of service construction

Because MyData is open source, developers can build access and services through public programming interfaces and libraries. Consent permissions—protection, authorization, and control—are managed through interfaces and programming instances that are separated according to purpose and usage rights. As a result, new consent operators, services, and applications naturally evolve.

Flexible privacy monitoring

Privacy is always protected because personal data moves between sources and sinks only with MyData operator permissions. In addition, MyData account management is separated from consent services and dataflows. The operator never stores any personal data generated by any source but acts only as a trusted consent manager and exposes the rights or limits to the use of an individual's data, on behalf of that individual. These flexible monitoring and governance mechanisms contrast sharply to existing models, in which consent is given on a service-by-service basis or through a single service operator. To our knowledge, PRIAAS combined with MyData is the most comprehensive solution to date in providing informed consent management for healthcare data use. A 2015 literature review found no single solution that addressed even the majority of informed consent issues,[6] but it predates the development of the ForgeRock Identity Platform (www.forgerock.com/platform), which addresses evolving customer data privacy regulations based on the UMA protocol. We believe that this platform is the only comparable solution to PRIAAS and MyData in massively distributed private data environments.

More efficient authorization

PRIAAS borrows naming conventions from the UMA protocol, such as Protection API, Authorization API, and uses the concept of the resource set. However, PRIAAS does not conform to UMA protocol flow. Our authorization is based on a centralized authorization server similar to UMA, but because resource servers and clients are always discoverable and trusted, our authorization flow requires fewer messages

compared to full UMA flow. For example, there is no longer a need to introduce the parties to each other in the beginning of authorization.

The authorization mechanism in PRIAAS is similar to OAuth 2.0 authorization code flow model because communication is expected to happen only between secure servers. However, PRIAAS differs in the way it defines the resource sets to be authorized: Instead of initiating registration by the resource server before the transaction, as in the OAuth 2.0 authorization flow, in PRIAAS, the resource owner initiates registration at the time of authorization transaction.

Conformance with emerging regulations

One major advantage of PRIAAS and MyData is conformance with regulations like the GDPR, which emphasize ease of use and interoperability. By brokering sources and sinks, the MyData operator enables trusted transfer of data and consent information with fewer messages, and the MyData account serves as a single hub for personal data management, allowing individuals to view, manage, and control their consents easily in a transparent and standardized way. Such standardization also facilitates interoperability.

Cost savings

Informed consent is considered valuable because it promotes trust in healthcare, which in turn ensures that people use healthcare more effectively.[7] Making consent safer and more efficient can reap even greater savings. Moreover, consent-management solutions like PRIAAS and MyData reduce the administrative time of medical personnel, who must otherwise process paper or online consent forms. Potential long-term profits stem from increased patient load and higher per-patient revenue or decreased per-patient cost.

The reduced learning curve is also a source of savings, as any new service investment has immediate costs in purchase, adaptation to the local organization, and staff training. MyData and PRIAAS are open source, which saves purchasing costs.

Finally, a comprehensive consent-management solution like MyData and PRIAAS promotes interoperability and reduces redundant documentation. Widespread adoption could move form system connectivity to interoperability among organizations and regions. The highest cost savings will come when a nation's health information systems are entirely interoperable. For example, complete interoperability within US health information systems has been estimated to yield savings of $77.8 billion annually.[8]

Improved health

Interoperability and cost savings are enablers that make personal data use rights a controlled, but ubiquitous service. Greater trust in healthcare services leads to benefits that directly improve health, such as easier communication among patients with similar health problems and the discovery of clinical trials.[9]

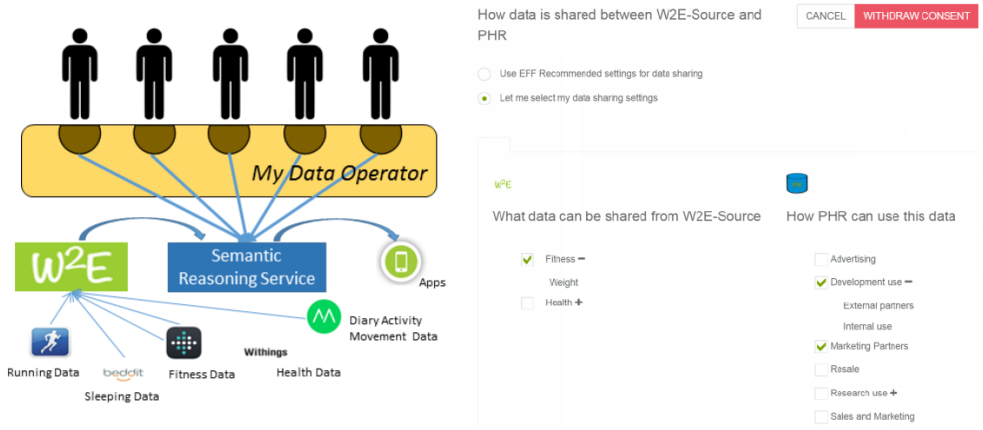
Sample Implementation

To validate the feasibility of PRIAAS, we developed a proof-of-concept implementation

in which users authorize data sinks and sources to exchange data in a secure and trusted manner.

Data exchange

Data is exchanged only between sources and sinks through common data APIs, and consent is transmitted between operator and sink and operator and source. We divided the proof-of-concept implementation into separate parts: one each for MyData operators (one or more), sources, and sinks. Each part has distinct and interoperable roles and responsibilities in consent management that comply with regulations such as GDPR. The individual with a MyData account can complete all actions needed to establish consent for personal data to flow from a source to a sink. MyData-compliant sources provide data in a machine-readable format (JavaScript Object Notation) through RESTful interfaces.



(a) (b)

Figure 4. PRIAAS and MyData implementation that involves multiple provider services and (b) an interface to manage consent for data use, in this case, to share fitness data with a personal health record (PHR).

Our implementation involved a health and wellness recommendation service that is based on multiple data sources. As shown in Figure 4a, the MyData operator manages user consent and data authorization by interacting with W2E, a general platform that aggregates wellness data platform (https://w2e.fi/frontpage), and components of the semantic reasoning service. Users must have an account at each of these services. The combination of W2E in MyData and the semantic reasoning service preserves privacy through pseudonyms and the separation of consent flow and dataflow. The W2E proxy accesses data from multiple sources that are not MyData compliant—mostly the backend servers of health and wellness device manufacturers—and delivers the data to the semantic reasoning service. Data delivery is subject to the MyData operator, which

manages the user's consent registry.

Figure 4b shows a screenshot of the consent-management interface, through which users connect sources and sinks and specify how the data sources can be used. In the screen portrayed, the user wants to share his fitness data from W2E with a Personal Health Record (PHR). Hence, PHR can fetch this data from W2E and use it in a way that benefits the user, such as giving his medical care providers more insight as well as supporting decisions relating to his health and healthcare.

Semantic reasoning

The reasoning service performs inference tasks based on ontologies and rules and makes health and wellness recommendations to user applications through an API. The recommendations result from a rule set, such as that in Table 1, which is drawn from publicly available Finnish healthcare guidelines. The rules infer a person's overall health, diabetes risk, and stress level from data fetched from multiple data sources. The semantic reasoning service can be maintained by officially authorized organizations that guarantee the validity of a data-driven reasoning service for third-party applications that interact with the user, such as a FitBit for fitness data.

Table 1. Sample rules for inferring health-related conditions in the semantic reasoning service.

Fact	***Clause***
TotalExercise	Exercise hasTimeStamp between(x,y) ∩ hasDuration ?d →TotalExercise hasDuration sum(?d) ∩ hasMeasurementDuration(y-x)
LowExerciseAmount	TotalExercise hasDuration ?d ∩ hasMeasurementDuration ?md ∩ ?d/?md < 0.04 → LowExerciseAmount
EnoughIntense Exercise	Exercise rdf:type IntenseExercise hasTimeStamp between(x,y) ∩ count>3 ∩ sum(hasDuration)/hasMeasurementDuration > 0.0074 → EnoughIntenseExercise
BMIIndex	(Weight/Height^2)*703 ?bmi → BMIIndex hasBMI ?bmi
Obesity	BodyMassIndex > 29.9 → Obesity
EfficientSleep	SleepEfficiency > 84 → EfficientSleep
OptimalBP	SystolicBloodPressure < 120 ∩ DiastolicBloodPressure < 80 → OptimalBP
HypertensionDeg1	159 > SystolicBloodPressure > 140 ∩ 99 > DiastolicBloodPressure > 90 → HypertensionDeg1
DiagnosedHypertension	(HypertensionDeg1 ∪ HypertensionDeg2 ∪ HypertensionDeg3) hasTimestamp between(x,y) ∩ avg(hasSystolic) > 140 ∩ avg(hasDiastolic) > 90 → DiagnosedHypertension
UnhealthyDiet	Purchases hasTimestamp between(x,y) ∩ rdfs:subClassOf Fruits_Berries_Vegetables count+1 ∩ count < 2TimesPerWeek → UnhealthyDiet
VeryHighType2DiabetesRisk	Age>64 ∩ Obesity ∩ DiagnoseHighBP ∩ (NotEnoughIntenseExercise ∩ NotEnoughModerateExercise) ∩ FamilyMember hasDiagnosedDiabetes ∩ HighBloodGlucose ∩ UnhealthyDiet → VeryHighType2DiabetesRisk
OptimalHealth	Normalweight ∩ (EnoughIntenseExercise ∪ EnoughModerateExercise) ∩

	NormalBP ∪ OptimalPB ∩ EfficientSleep → OptimalHealth
Stressed	HypertensionDeg1 ∪ HypertensionDeg2 ∩ InefficientSleep hasTimestamp between(x, y) → Stressed ∩ Relax
ReduceTraining	Underweight ∩ HighExerciseAmount ∩ Stressed → ReduceTraining
HealthyDiet	Overweight ∩ LowExerciseAmount → Healthy Diet ∩ MoreTraining

Figure 5 depicts the MyData core operations for establishing trust between the components that together realize the recommendation service. Both the health application and Semantic Reasoner have consent tokens to establish the trust required for data exchange. In the scenario in Figure 5, Semantic Reasoner separates user applications from the aggregated personal data and helps preserve the original data from exploitation by third-party applications.

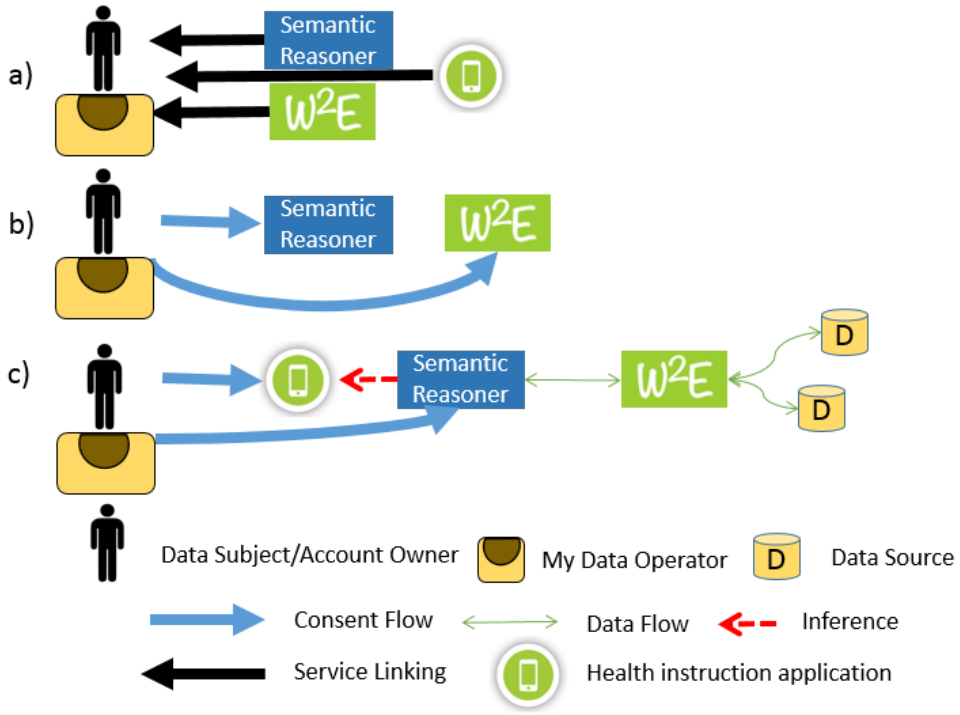


Figure 5. MyData operations for inferring health-related conditions from wellness data. The process to establish inference operations has three steps in which the user (a) links Semantic Reasoner (a health application) and the W2E aggregator service to his MyData operator account; (b) authorizes Semantic Reasoner to access his health data from the W2E aggregator service; and (c) authorizes the linked health application to use data from Semantic Reasoner for health-related guidance

As this implementation shows, PRIAAS and MyData facilitate and expedite the creation of new services, create data bindings between actors, and promote new business models to reuse-refine-reuse personal data within both the individual and group domains, with the goal of creating novel services and applications that enhance wellbeing.

Together, PRIAAS and MyData provide a holistic solution for consent delivery and management. Individuals have tools to manage their data as well as innovative services. Companies benefit from the new data-based business opportunities, and standardization enables interoperability and lowers the barrier for new companies and businesses to enter the healthcare-support market. Society benefits from the new services as well as standardized structures, processes, and policies that address individual rights to control data use.

PRIAAS and MyData focus on consent management for two reasons. First, consents are the backbone of any legislative framework that defines information processing from a human-centric perspective. Second, standardized consent that is both human and machine readable unites data management systems, legislative frameworks, and individual needs. These reasons suggest applications beyond healthcare. Indeed, with minor modifications, PRIAAS and MyData could be the basis for a consistent data collection and processing approach regardless of domain.

Acknowledgments

This research has been supported by a grant from Tekes–the Finnish Funding Agency for Innovation as part of the Digital Health Revolution program.

References

1. "Reform of EU Data Protection Rules," European Commission, 2 Aug. 2016; http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

2. A. Poikola, K. Kuikkaniemi, and H. Honko, "MyData—A Nordic Model for Human-Centered Personal Data Management and Processing," white paper, Open Knowledge Finland, Finnish Ministry of Transport and Communication, 2015; http://urn.fi/URN:ISBN:978-952-243-455-5.

3. J. Kaye et al., "Dynamic Consent: A Patient interface for Twenty-First Century Research Networks," *European J. Human Genetics*, vol. 23, no. 2, 2015, pp. 141–146.

4. T. Hardjono et al., *User-Managed Access (UMA) Profile of OAuth,* v. 2.0; specification by User-Managed Access Work Group, Kantara Initiative, 28 Dec. 2015; https://docs.kantarainitiative.org/uma/rec-uma-core.html.

5. *Kantara Initiative: Minimum Viable Consent Receipt Specification*, v. 0.7, 2015; https://github.com/KI-CISWG/MVCR.

6. R. Arnold, A. Hillebrand, and M. Waldburger, *Personal Data and Privacy*, Ofcom, 2015; http://stakeholders.ofcom.org.uk/binaries/internet/personal-data-and-privacy/Personal_Data_and_Privacy.pdf.

7. R. Roache, "Why Is Informed Consent Important?" *J. Medical Ethics*, vol. 40, no. 7, 2014, pp. 435–436.

8. J. Walker et al., "The Value of Healthcare Information Exchange and Interoperability," *Health Affairs*, vol. 24, no. 1, 2005; http://content.healthaffairs.org/content/early/2005/01/19/hlthaff.w5.10.

9. R. Steinbrook, "Personally Controlled Online Health Data—The Next Big Thing in Medical Care?" *New England J. Medicine*, vol. 358, no. 16, 2008, pp. 1653–1656.

Xiang Su *is a post-doctoral researcher in computer science in the Center of Ubiquitous Computing at the*

University of Oulu. His research interests include semantic technologies, the Internet of Things, knowledge representations, and context modeling and reasoning. Su received a PhD in technology from the University of Oulu. He is a member of IEEE. Contact him at xiang.su@ee.oulu.fi.

***Jarkko Hyysalo** is a postdoctoral researcher in the Faculty of Information Technology and Electrical Engineering at the University of Oulu. His research interests include software architectures and processes and collaborative work. Hyysalo received a PhD in information processing science from the University of Oulu. Contact him at jarkko.hyysalo@oulu.fi*

***Mika Rautiainen** is a post-doctoral researcher in the Faculty of Electrical and Information Engineering at the University of Oulu. His research interests include content-based multimedia retrieval and management systems, scalable data-processing architectures, cognitive user experience, pattern recognition, digital image and video processing, and understanding. Rautiainen received a PhD in technology in computer science from the University of Oulu. Contact him at mika@valossa.com.*

***Jukka Riekki** a professor of software architectures for embedded systems and dean of the Faculty of Information Technology and Electrical Engineering at the University of Oulu and a principal investigator in the university's Center of Ubiquitous Computing. His research interests include interactive, context-aware systems that support everyday tasks and edge computing driven by the Internet of Things (IoT). Riekki received a PhD in technology from the University of Oulu. He is a member of IEEE. Contact him at jukka.riekki@oulu.fi.*

***Jaakko Sauvola** is a professor of data-intensive systems and advanced software at the University of Oulu and leader of Finland's High-Tech ICT Leverage from Long-Term Assetization (HILLA) Program. His research interests include mobility, system architectures, and data-intensive services and analytics. Sauvola received a PhD in technology from the University of Oulu. Contact him at jaakko.sauvola@oulu.fi.*

***Altti Ilari Maarala** is a doctoral student in the Department of Computer Science at Aalto University. His research interests include the IoT, big data, semantic technologies, knowledge representation, parallel algorithms, and computational genomics. Maarala received an MSc in computer science from the University of Oulu. Contact him at ilari.maarala@aalto.fi.*

***Harri Hirvonsalo** is an MSc student in the Faculty of Information Technology and Electrical Engineering (ITEE) at the University of Oulu. His research interests include software architectures, security and privacy, and personal data and identity management. Contact him at harri.hirvonsalo@oulu.fi.*

***Pingjiang Li** is an MSc student in the Center of Ubiquitous Computing at the University of Oulu. His research interests include ubiquitous computing and human–computer interaction. Li received a BS in computer science from the University of Jinan. Contact him at Pingjiang.Li@student.oulu.fi.*

***Harri Honko** is a track lead in technology and regulation in the digital health revolution program and project manager in the Personal Health Informatics group at the Tampere University of Technology. His research interests include identity, authorization, and consent management technologies; system architectures; and regulation for personal data management. Honko received an MSc in electronic engineering in Tampere University of Technology. He is a society affiliate of IEEE. Contact him at harri.honko@tut.fi.*

<begin sidebar>

Guiding Architectural Principles

We inherited our privacy-as-a-service (PRIAAS) architectural requirements from extended MyData principles augmented with the General Data Privacy Regulation (GDPR). We view these principles as foundational to human-centric data processing and personal information management.

- **Control.** Individuals have the right and practical means to manage their data and privacy according to the GDPR.
- **Access.** Data must be easy for the individual to access and use
- **Translation.** There must be a way to convert data from single entities into a meaningful, machine-readable resource that can be used to create new services;
- **Interoperability.** To support an open business environment, the shared data infrastructure must enable the coordinated management of personal data, ensure interoperability, and facilitate the compliance of various entities to stricter data protection regulations.
- **Provisioning.** The infrastructure must allow individuals to change service providers and control their data management.