Technical Specification

ISO/TS 6201

Health informatics — Personalized digital health framework

Informatique de santé — Cadre de santé numérique personnalisé

First edition
2025-02

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

Reference number
ISO/TS 6201:2025(en)

© ISO 2025

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO’s member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

© ISO 2025 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

© ISO 2025 – All rights reserved

Introduction

Developments in information and communication technology (ICT) have enabled data to be collected from individuals in a variety of ways. Various health-related data not only facilitate finding effective treatment strategies but also establishing personalized healthcare services, as Figure 1 depicts. Therefore, the concept of digital healthcare has emerged. Digital healthcare can be defined as comprehensive medical services that utilize an individual's health-related data, including personal health data that may be collected from devices, platforms and applications.

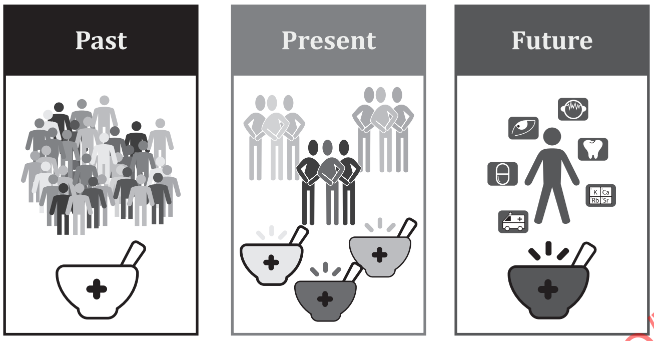


Figure 1 — Evolution in personalized digital health

Tremendous amounts of information can be produced by individuals, such as eating habits, exercise, hours of sleep, and also health records. This information is considered along with physical, social, and mental characteristics of individuals and can result in different treatment options and prescriptions. Accordingly, personalized digital health (PDH) refers to electronic services that support the health of individuals when they can add to and handle their own health information.

Existing medical care procedures focus on suggesting medical solutions when a disease occurs. Digital health goes beyond that scope and supports an individual's decision-making process by providing the most appropriate advice based on their continuously generated health-related data. Personalized digital health aims to go one step further, enabling an individual to identify and eliminate the potential causes of disease before they occur.

Another goal of digital healthcare is to effectively monitor and manage personal health by using platforms and applications that can provide personalized healthcare services. The personalized services are based on an individual's health information, including biometric information and family medical history, which are stored in large databases.

Personalized digital services based on a combination of medical knowledge and IT solutions can improve healthcare. If personalized digital health becomes the norm, a PDH service could utilize a patient's genomic information to help find the most appropriate drugs and treatment methods. This can be significantly enabled by collecting, categorizing or "tagging", and storing patients' biometric information, medical documentation, genetic analysis, smart or wearable device information, family history, and clinical examination information.

Medical data, previously managed by hospitals and institutions, are now being transformed and integrated into PDH platforms, a concept that empowers individuals to be the decision-makers of their own health information and data use. Therefore, PDH data comprises both health records from hospitals and health professionals, and personal health data generated by smart devices.

When individuals are given the right to decide how their health data is handled or managed, a consent system for their personal information is necessary. A consent system is a system in which individuals can actively manage their consent at any time. Many people have given permission to use their personal information to medical care institutions and other organizations. Traditionally, a paper-based agreement was widely used. Nowadays, the number of medical institutions using digital contracts is rising because of the wide usage of smartphones and PCs. However, since these methods are conducted on a one-off basis, it is difficult to modify or withdraw the consent once it is given.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

© ISO 2025 – All rights reserved

Dynamic consent is a form of consent that allows people to decide whether to provide specific information via interactive digital interfaces. This agreement method was first implemented in biomedical and genomic studies that required continuous contact with participants. Dynamic consent gives individuals more autonomy by giving them the power to control their own data. A customized interface that enables two-way communication between healthcare providers and users is important for dynamic consent to work effectively.

Various stakeholders, such as researchers, healthcare providers, institutions and governments, can access individuals' health data through an efficient and dynamic consent system. To reach the full potential of PDH services, quickly establishing standards for systems, infrastructure, platforms and frameworks is imperative. Supporting personalized knowledge representation and related ontologies is mandatory when seeking to transform how individuals manage their healthcare, and it can only be realized with PDH technology. Otherwise, data integration is almost impossible, and failure of data management can hold back the development of a successful digital health system.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

© ISO 2025 – All rights reserved

Health informatics — Personalized digital health framework

1 Scope

This document specifies a framework for the interoperability of services and information tailored towards personalized digital health informatics. It establishes a common set of requirements and data specifications necessary for multi-level interoperability, as well as for dynamic consent and knowledge sharing.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
consent
freely given agreements based on adequate information obtained prior to the collection/use of participant data

[SOURCE: ISO 20252:2019, 3.20]

3.2
dynamic consent
consent (3.1) that enables communication between owners of the data and their consumers via digital interfaces during the process of utilizing health data

3.3
interoperability
ability of two or more systems or components to exchange information and to use the information that has been exchanged

[SOURCE: IEEE[10]]

3.4
personalized digital health
PDH
electronic services that support health of individuals when they can add and handle their health information

3.5
personalized digital health framework
PDHF
framework for the interoperability of services and information, tailored towards *personalized digital health* (3.4) informatics, that establishes a common set of requirements and data specifications necessary for multi-level interoperability, as well as for dynamic consent and knowledge sharing

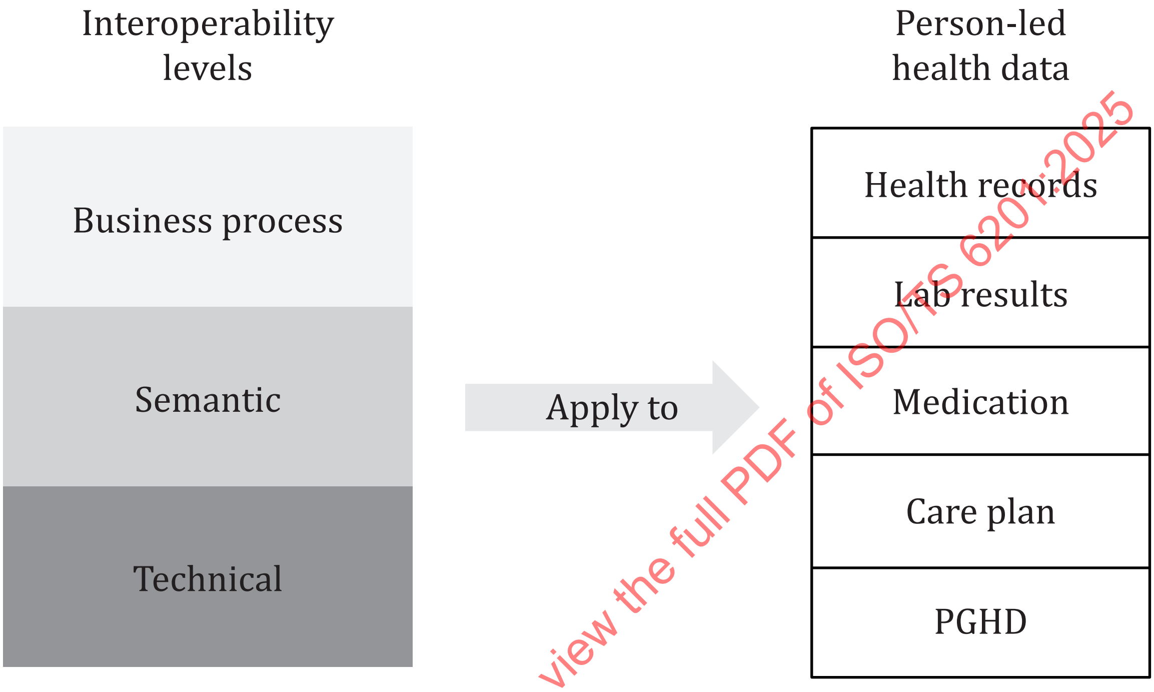
STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

© ISO 2025 – All rights reserved

4 Person-led health and personalized digital health record

4.1 General

Because of the increasing need for person centred care, there are several possible approaches to provide the required healthcare, facilitating patient independence and self-care. Person-led health supports self-care using data such as health records, lab results, medication, care plan, and person generated health data (PGHD). On the other hand, several interoperability levels can be identified, such as business process, syntactic and semantic ones, which apply to the person-led health data, as depicted in Figure 2.



STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

Figure 2 — Interoperability levels and person-led health data

The personalized digital health framework (PDHF) specified in this document provides a solution to person centred care. This PDHF achieves several objectives:

- facilitating interoperability between different healthcare institutions' information systems;
- integrating PGHD, coming from personal devices like smart watches, into existing healthcare institutions information systems;
- facilitating the creation of personalized digital health records (PDHR) managed by individuals, where medical information coming from different sources can be combined, including both PGHD and health data coming from medical institutions;
- facilitating patients' consent management through the PDHR, by allowing them to easily decide who can access their medical information and to keep track of their data.

4.2 Personalized digital health record (PDHR)

A personalized digital health record (PDHR) combines medical data, such as health records, lab results, medication and treatments received by an individual from medical institutions, with person generated health data (PGHD), acquired using wearables, smartphones or IoT devices, during daily life.

On the one hand, such heterogeneous data should be modelled to facilitate interoperability and secured to protect patient's privacy. On the other hand, there is a need for services and applications that provide the required interoperability and security.

PDHR supports PDHF to:

- define interoperable data models, for both medical institutions' data and PGHD;
- provide protection and access control to medical data;
- provide search capabilities.

4.3 Interoperability issues

Digital transformation within the health domain has made it possible, for different stakeholders in the healthcare domain, to collect and store health-related data by using a variety of health information technologies. Guaranteeing interoperability is very important as the demand for reusing and reanalysing personal health data increases. Stakeholders involved in the use of personal health data vary, and include data owners, hospitals, pharmacies, medical service providers, researchers and manufacturers. To meet the needs of different stakeholders, the exchange of health data should be seamless across different institutions as well as different regions and even different countries, and the exchanged health data should be interpreted in the same way anytime, anywhere.

The key point of the personalized digital health framework (PDHF) lies in the combination of personal health data that are physically distributed. As more data get connected, more information is available for analysis and prediction. Information related to individual health is stored in different formats, both in medical institutions, such as hospitals and pharmacies, and in wearable devices and mobile application servers. Smooth exchange of personal health data between different countries requires access to interoperability in a multifaceted view, including technical aspects such as system interfaces and communication protocols, to ensure consistent interpretation of exchanged data.

Interoperability issues exist at different levels, as shown in Figure 3.

There are different health data sources that inject healthcare data into a health data repository. To harmonize the information contained inside this repository, two types of interoperability are considered: one concerns terminology and the other concerns information structure.

Terminology interoperability ensures identical data interpretation in different institutions, regions and countries, mainly dealing with terminology and ontology within the health domain. Identification of medicinal products (IDMP), SNOMED-CT[1], and Logical Observation Identifiers Names and Codes (LOINC)[2] are notable examples that focus on semantic interoperability.

Information structure interoperability refers to the format of health data exchanged between different institutions or the interoperability between structures. International standards development organizations, such as Health Level Seven (HL7)[3] and Integrating the Healthcare Enterprise (IHE)[4], have been developing various standards to support technical interoperability. Fast Healthcare Interoperability Resource (FHIR)[5], led by HL7, is a representative case of the next-generation health information framework, commonly used in the health domain, and defines the model as a resource unit to improve reusability and flexibility of the data model.

The business process level includes several services, such as access control, registration, consent or patient identity. These services use the health data repository to provide information to the users accessing through different applications. The objective of this level is to provide organizational interoperability, such as policies, regulations and laws between institutions that exchange health information. This level should be able to continuously reflect changing environments and policies. A typical example of organizational interoperability is defining overall business processes and workflows that are related to the registration of patients and health information, access control to health data or obtaining consent from individuals for accessing their health-related data.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

[1] https://www.snomed.org/

[2] https://loinc.org/

[3] https://www.hl7.org/

[4] https://www.ihe.net/

[5] https://hl7.org/fhir/

© ISO 2025 – All rights reserved

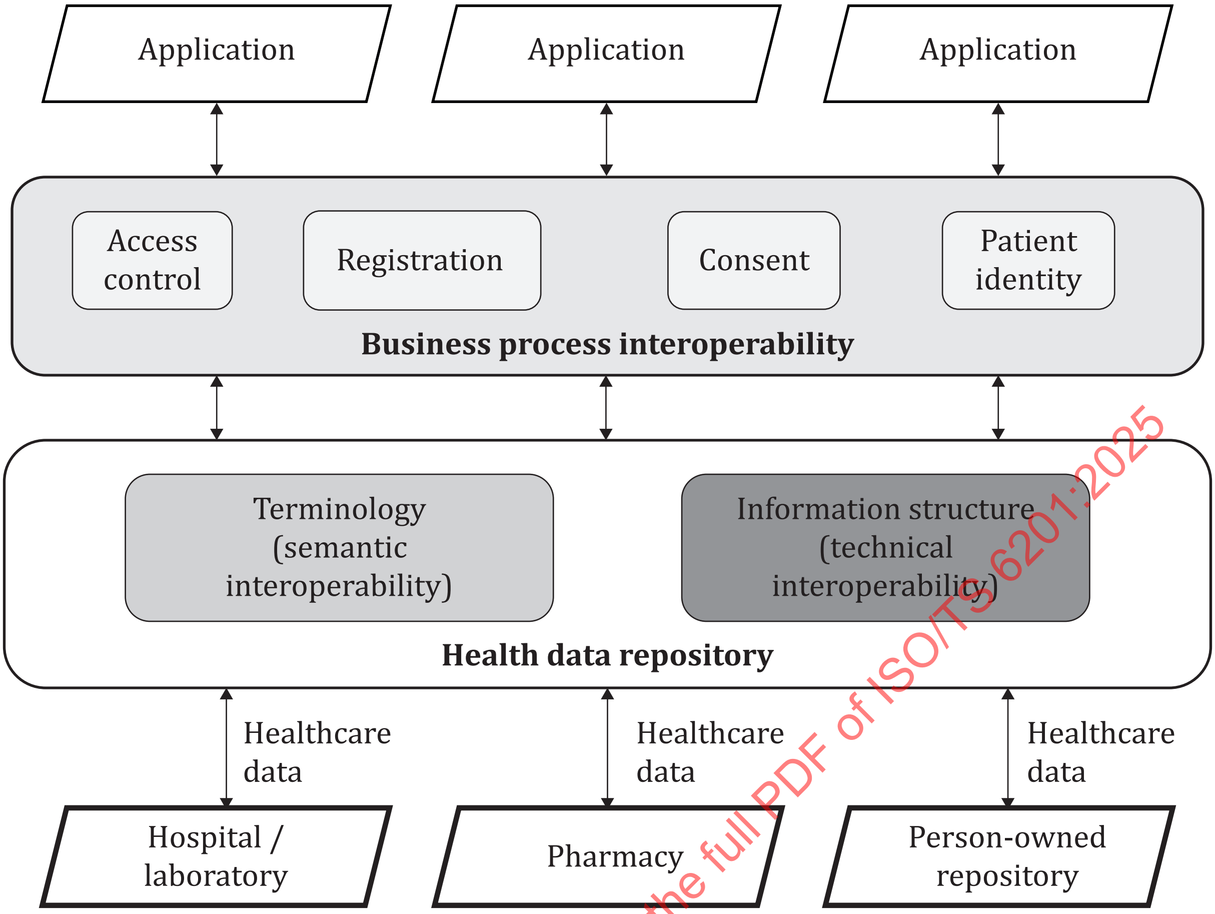


Figure 3 — Interoperability at different levels

Implementations of the personalized digital health framework should follow the structure of Figure 3 and implement some of the boxes included in that figure. One of the possible implementation approaches is described in 5.2.

5 Personalized digital health framework

5.1 General

The framework for personalized digital health (PDH) has several purposes:

- to provide a common structure and model for the development of the PDH standards;
- to allow organizing the functionality of PDH systems in an independent an interoperable way;
- to describe components and interactions between digital health systems;
- to facilitate alignment with other initiatives at different levels (countries, standardization bodies, public institutions worldwide, etc.).

There are different possible approaches for implementing a PDHF. The next subclause describes one of them. This approach provides interoperability, security, access control and support for different medical content types with the use of a modular architecture consisting of several services to guarantee that the access to medical information is only given to authorized parties.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

5.2 Personalized digital health framework (PDHF) description

The modules forming part of the generic architecture, depicted in Figure 4, are based on the use of an application programming interface (API) against web services.

The different modules and their functionalities are the following (ordered alphabetically):

- Authorization service: module for access authorization based on privacy and access rules, and for validation of medical consents.
- Health content service: module in charge of health information management, both in reading and writing operations. It covers the different formats of the medical information.
- Metadata service: module in charge of handling metadata of medical documents, which can help in identifying and finding them.
- Protection service: module which creates protection to information and applies the mechanisms defined (i.e., encryption, signature).
- Report service: module in charge of reporting the operations done in the system, especially those not authorized.
- Rule service: module in charge of the creation of the authorization rules, which are organized into policies. It is also in charge of the creation and management of consent.
- User application: application that sends requests to the workflow manager based on user actions. The communication between this application and the rest of the architecture is done through a secure channel.
- Workflow manager: intermediate module that acts as a unique entry point to the system. It checks operation authorization before interacting with other modules.

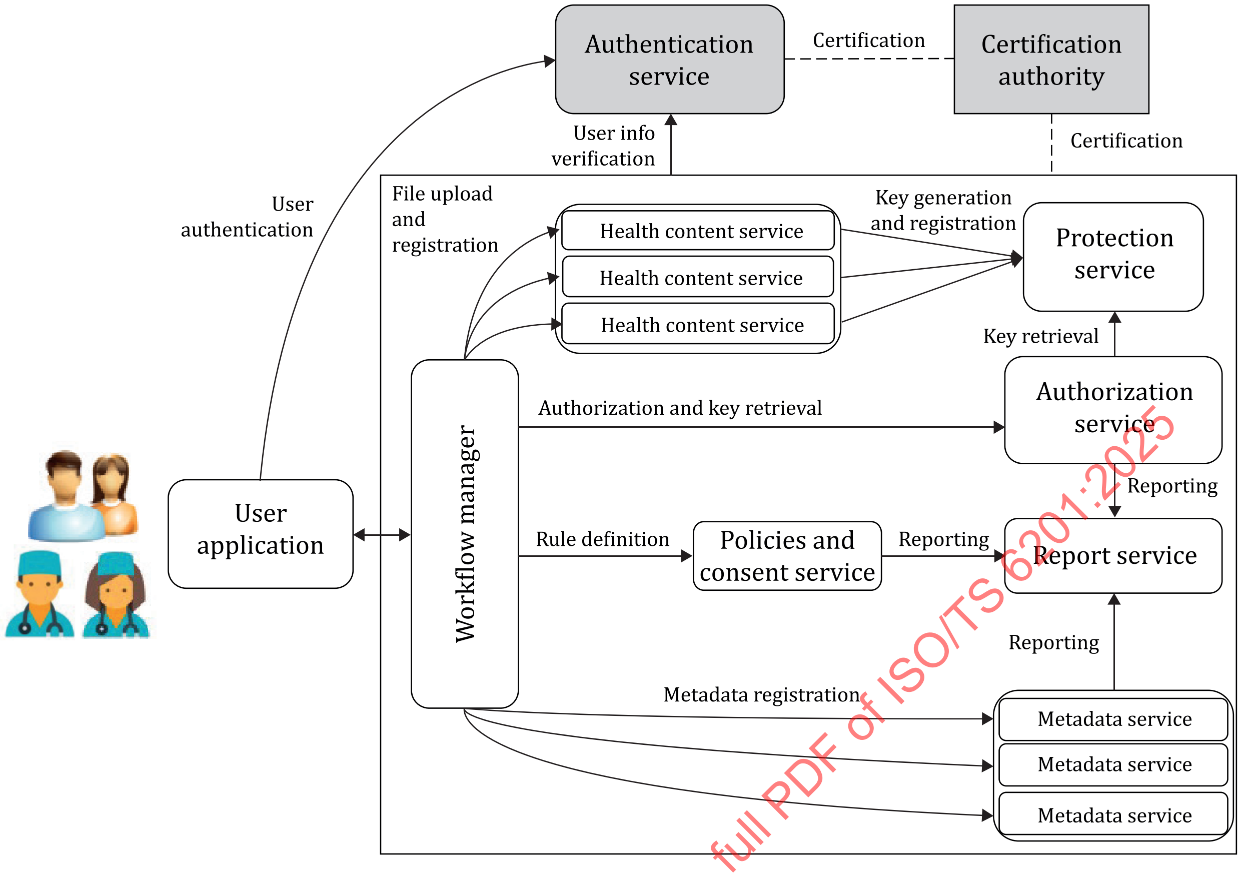
The external modules are:

- Authentication service: it provides user identification. Its implementation should be based on standards such as OAuth 2.0,[1] JSON Web Tokens[2] or OpenID Connect[3].
- Certification authority: it provides digital certificates to secure communications.

This architecture allows the simultaneous use of different formats representing medical information. These formats are managed by health content and metadata services. As Figure 4 shows, health content and metadata services can contain several submodules to provide different formats supported by the system implementing this architecture. The architecture also allows the inclusion of new modules, such as search service, to provide search capabilities.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

© ISO 2025 – All rights reserved



Key

▨ external modules, not to be standardized

□ modules to be standardized

Figure 4 — A reference architecture

Annex A describes three use cases to show how the different modules of this architecture interact. Use case 1 shows how to register medical information, while use case 2 shows the registration in a secure environment. Use case 3 presents how content is consumed with secure access to medical information.

6 Dynamic consent

Dynamic consent is an agreement method that enables two-way communication between data providers (owners of the data, i.e. patients) and consumers via a digital interface during the process of utilizing personal health data. Non-dynamic consent does not allow changes and does not force communication back to the data owner. In some cases, non-dynamic consent on health data is for a short-term or one-time use cases, such as providing data to insurance claims or specific studies.

Consent involves at least a data provider, who shares their data, and a data consumer, who accesses those data. Optionally, a third actor (an intermediary) is the one that collects the consent from the data provider and manages the consumption of data by different data consumers. The consent is signed by the data provider and, optionally, by either the data consumer or the intermediary.

Consent characteristics include:

- Informed: the consent provider is clearly informed about what is consented.
- Broad: it uses ambiguous information with the objective of flexibility in the use of the consent.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

- Explicit: all details and scope are provided.
- Specific: it only applies to a reduced and limited context.
- Dynamic: it provides two-way communication between data providers and data consumers.

Consent mechanisms should provide:

- clarity on whether individual consent to the processing of their personal health data is required, and, if so, the criteria used to make this determination;
- information on what constitutes valid consent and how consent can be withdrawn;
- lawful alternatives and exemptions to requiring consent, including in circumstances where obtaining consent is impossible, impracticable or incompatible with the achievement of the health-related public interest purpose, and the processing is subject to consistent safeguards.

In the health domain, to ensure the autonomy of information subjects with respect to the utilization of personal health data, informed consent that is agreed upon after a sufficient understanding of the purpose and scope is considered an important step. However, with technological advances in digital health, the scope of application has also expanded in medical treatment, disease prediction, symptom analysis, new drug development, cohort research, etc., away from only providing historical data or static research. As a result, different consent types can be needed in different applications.

As an example of broad consent, in the case of research using human-derived materials, such in biobanks, it is possible that donors do not know exactly for what purpose and where the materials will be used at the time of donation. Nevertheless, biobanks provide anonymized human-derived materials when researchers request data, and researchers do not know where it was originated. Therefore, biobanks mainly use a broad consent approach that agrees that donor human derivatives can be used for a wide range of research approved by institutions based on an application form.

In addition, the support of various types of consent reflects individual preferences. Dynamic consent provides users with a variety of options to let them manage their own data with flexibility and individual autonomy, and it supports continuous two-way communication between data providers and consumers on a digital basis. This is a way to maximize autonomy for those who want to actively utilize their health data. However, continuous communication and selection can lead to consent fatigue and, in the worst case, to a decline in participation. Dynamic consent also enables selective participation using various consent models to respect the autonomy of those who prefer to participate passively. This method of consent can be changed whenever the participant wants, and it is also possible to actively join in only certain areas of interest. For example, if chronic patients with asthma agree to utilize their data in multiple places and only prefer to receive information regarding how their derivative data is used in asthma research, the results can be filtered based on these preferences, and broad consent may be applied to the rest of the research.

The life cycle of personal health data utilization has changed to a more long-term form, even longer than a lifetime. Therefore, flexibility in the process to obtain consent is necessary. Traditional consent methods involve one-way communication, with data providers usually giving consent to data consumers, but not vice versa. Moreover, with traditional consent methods, including paper-based ones, the process to revise one's consent is sometimes onerous because of the additional steps that both data providers and consumers should take. If the person does not have access to all the details of the agreement, a withdrawal process cannot be performed, and going through all the terms of the contract is a tedious task. It can also be difficult for individuals to remember what agreements they have made. The personalized digital health framework (PDHF) requires consent that allows individuals (data owners) to take the initiative to participate in their health data sharing environment with data ownership. Because of the fast-changing environment, a flexible model for consent process is essential. By providing individuals with various options regarding data provision and consent, dynamic consent can expand individual autonomy and thus support an individual-driven health data environment.

Features of dynamic consent include:

- It allows continuous and long-term updating and communication of the relationship between data provider and data consumer.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

- It monitors data life cycle, including who accessed the data and when, so data providers receive information on the use of their data and the results (or outcomes) of that use.
- It allows to be updated and even revoked at any time at the request of the data provider.
- Consent is conditional.
- Consent may be rules-based.
- Digital interfaces facilitate providing different types of consent, receiving information, and changing individual preferences.
- Dynamism is either explicit (selected by the provider) or implicit (specified in consent information).

Dynamic consent supports the interoperability levels of Figure 3.

In addition, dynamic consent is implementable with the architecture of Figure 4. Annex B shows two dynamic consent use cases.

Since big healthcare data is scattered in multiple places, there are some issues regarding healthcare data sharing. Patients should be able to dynamically give or retrieve their consent, and dynamic consent allows this by giving patients control of their data. Thus, by supporting dynamic consent, PDHF can ensure patients' control, and it can support patient-centred healthcare in three ways. First, the framework can provide data control to patients; second, PDHF can give autonomy to data providers (this is difficult to support in current systems due to the static or one-time consent method); finally, PDHF can provide a patient's consent history.

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

7 Personalized digital health patient journey

The patient journey describes a series of events, obtained from healthcare providers, that happened to the patients related to their health problems. It is partially based on Reference [4]. The concept of the patient journey is adopted in patient experience and patient safety to improve healthcare services. The patient journey covers different healthcare services depending on different perspectives, for example those of healthcare service providers or patients. From the perspective of a healthcare provider, the patient journey is a flow of healthcare services provided to the patients and is utilized to improve patient experience or workforce engagement.[5,6] From the perspective of a patient, the patient journey includes a wide range of healthcare service points, including treatments, prevention, and health promotion in various institutions.

Patient journeys consider that patients' needs can differ at different stages of the disease, for example at the time of initial symptoms vs. the time of treatment. Patient journeys also reflect patients' personal experiences, which vary depending on the person, health institution and country.

Considering these aspects, a basic patient journey structure for digital health services in the context of the personalized digital health records (PDHR) can be developed. In addition to the basic structure of the patient journey, which is applied regardless of disease, it is also possible to develop a disease-specific patient journey subject to several common chronic diseases. A patient journey mapping is the development of a disease-specific patient journey from a general patient journey structure.

Patient journeys differ by including distinct service components, depending on the perspectives of observing health services.

As shown in Figure 5, the general patient journey flow consists of four stages: prevention, diagnosis, treatment and maintenance. Other stages are also possible. In most cases, stages from different approaches can be mapped between the four main stages.

In the prevention stage, a person is in a healthy state and does not have any disease yet. Thus, the person has not made a visit to a healthcare provider or received any initial diagnosis. The awareness stage and the screening stage in the MAPS's (Mapping the patient journey towards Actionable beyond the Pill Solutions) patient journey[7,8] are matched to the prevention stage.

The diagnosis stage starts from a patient's first visit to a healthcare provider for diagnosis and ends when the patient receives treatment, which is the start of the treatment stage.

The treatment stage includes a series of healthcare services that aim for recovery and for the prevention of deterioration or disability. The treatment stage is the period for admission and outpatient service for treatment.

Lastly, the maintenance stage consists of follow-up, rehabilitation, or palliative care after active treatment for the disease. The maintenance stage continues until the death of a patient. A patient can directly enter the maintenance stage from the diagnosis stage when the patient gives up receiving medical treatment.

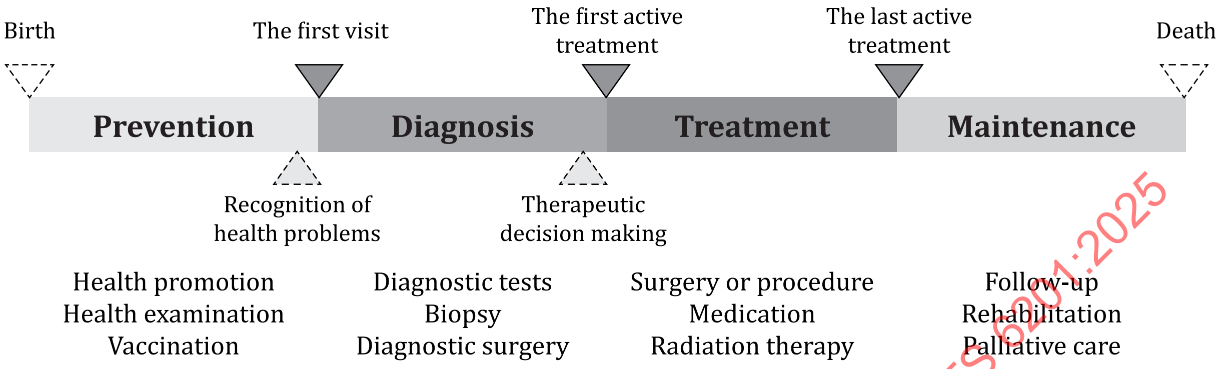


Figure 5 — General patient journey flow

Table 1 summarizes the four stages and provides some examples.

Table 1 — General patient journey and stage definition

Stage	Definition	Available services	Time duration	MAPS[a] patient journey
Prevention	A healthy state before the occurrence of disease	Prevention, health promotion, health examination, etc.	From birth to before the first visit to health providers for disease diagnosis	Awareness, Screening
Diagnosis	Including a series of services for diagnosis by visiting a healthcare provider after recognition of the disease	Diagnosis tests, biopsy, diagnostic surgery, complaints, current and past history, family history, etc.	From the first visit to a healthcare provider before getting active treatment	Diagnosis
Treatment	After the decision to treat, active treatment services, including operations, procedures, and medications to recover or prevent deterioration or disability	Surgery, procedure, medication, etc.	Duration for active treatment	Treatment
Maintenance	Follow-up, rehabilitation, and palliative care	Regular medical check-ups, physical therapy, etc.	After active treatment, until death	Awareness

[a] MAPS: Mapping the patient journey towards Actionable beyond the Pill Solutions

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

Annex A
(informative)

Implementation use cases of personalized digital health framework

A.1 General

This annex presents three use cases to show how the different modules of the architecture described in 5.2 interact. Use case 1 shows how to register medical information, while use case 2 shows the registration in a secure environment. Finally, use case 3 presents how content is consumed with secure access to medical information.

A.2 Use case 1: Registration of medical information

The use case shown in Figure A.1 represents the situation in which a user wants to create some medical content, which is not required to be protected. This is done to illustrate a simple scenario, but it is usually better to protect information as shown in Figure A.2.

First, the user has to authenticate in front of the Authentication Service in order to receive a valid token. This token will be used afterwards when invoking the rest of the services through the user application. It is worth noting that the services cannot be invoked directly but only through the workflow manager. Two services are used in this use case, health content service (HCS) and metadata service (MS). HCS is responsible for content creation and storage, while MS allows metadata registration.

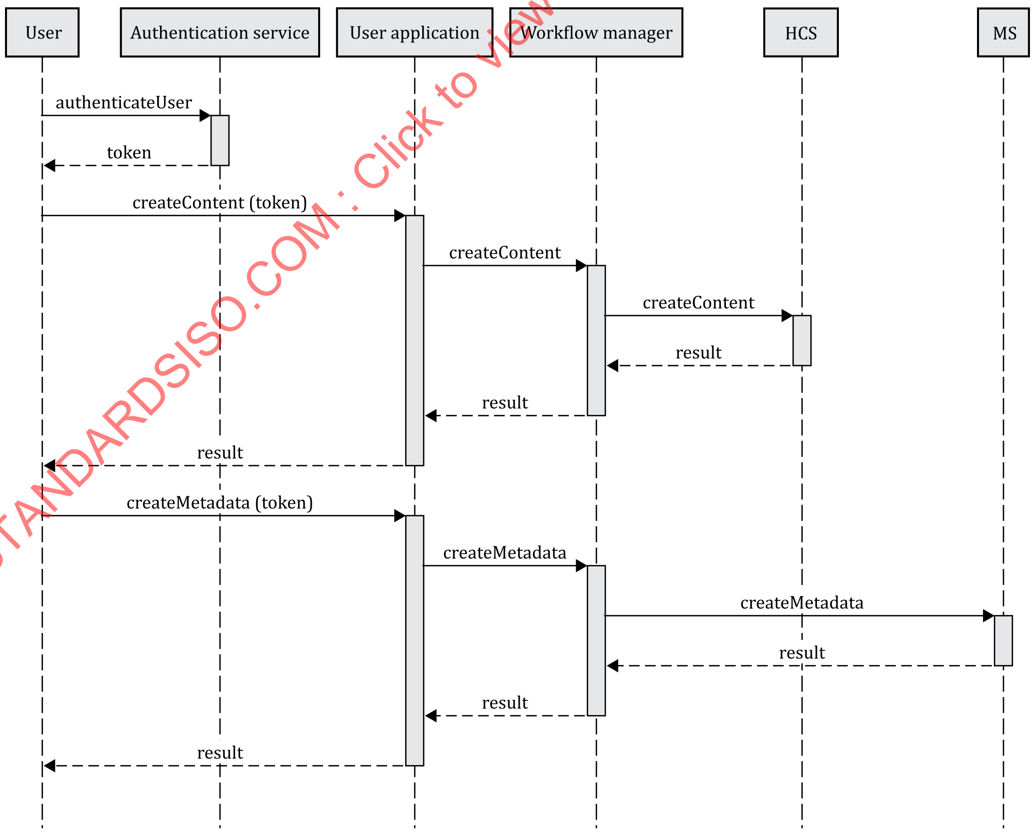


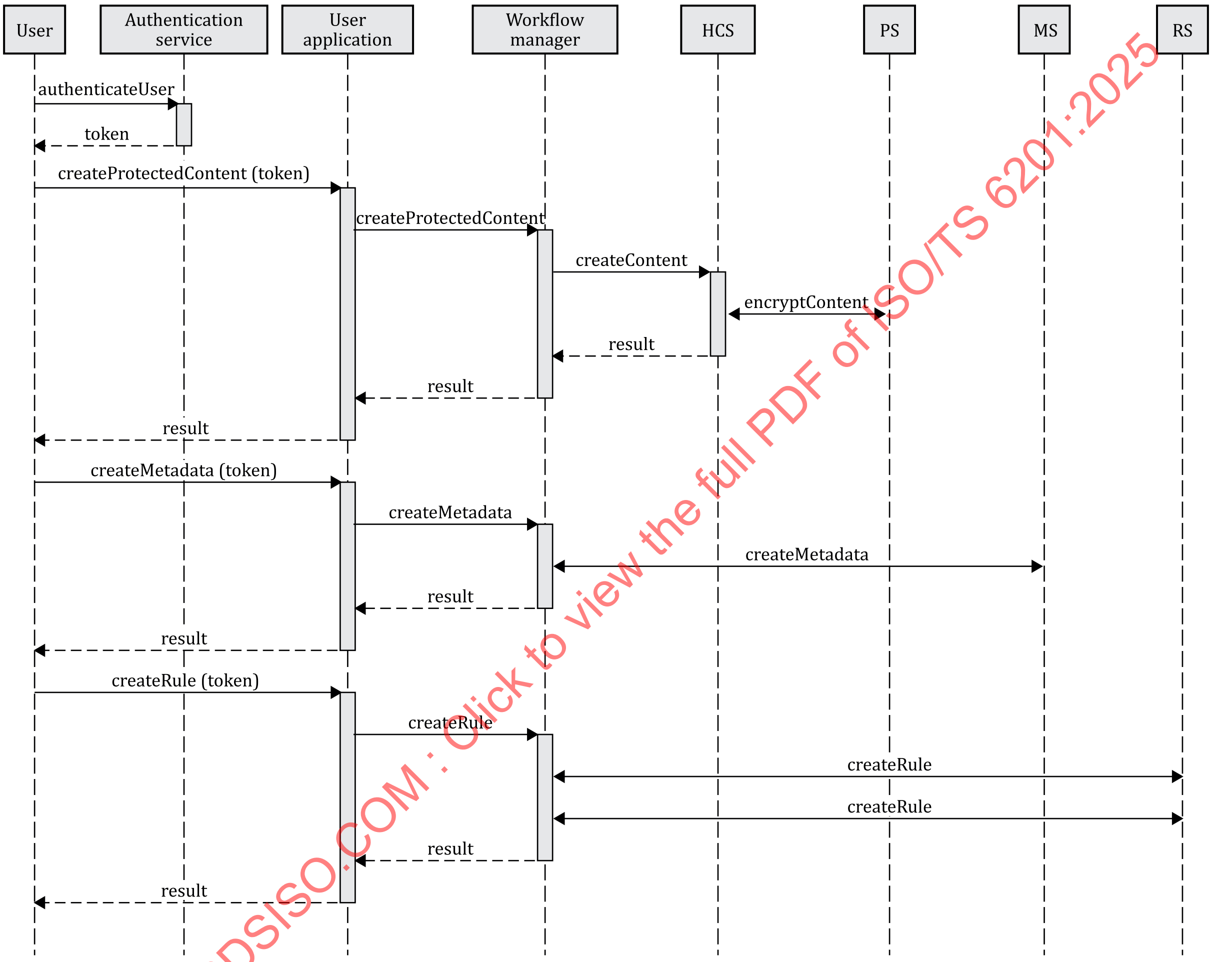
Figure A.1 — Simple registration use case

STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

A.3 Use case 2: Registration of protected medical information

The use case shown in Figure A.2 represents the situation in which a user wants to create some medical content that requires encryption and privacy protection, which is the most common situation.

As in use case 1, the first step is that the user has to authenticate in front of the Authentication Service in order to receive a valid token. This token will be used afterwards when invoking the rest of services through the user application. Aside from health content service (HCS) and metadata service (MS), in this use case two more services are used, protection service (PS) and rule service (RS). The PS is called from the HCS in order to encrypt the medical information stored. Afterwards, two privacy policies are created by the RS, to control access to the protected medical content.



STANDARDSISO.COM : Click to view the full PDF of ISO/TS 6201:2025

Figure A.2 — Protected registration use case

A.4 Use case 3: Secure access to medical information

The use case shown in Figure A.3 represents the situation in which a health professional wants to access some medical information a patient has shared with them. This is complementary to use case 2: in use case 3 the user wants to access protected medical information which was previously created by the user in use case 2.

As in use cases 1 and 2, the first step is that the user has to authenticate in front of the authentication service (AS) in order to receive a valid token. This token will be used afterwards when invoking the rest of services through the user application. The health professional asks for access to a protected content previously uploaded and protected using encryption mechanisms and privacy rules. This request is sent to the health content service (HCS), which, in turn, asks for authorization to the AS, which takes the existing access rules into account. In case of successful authorization, as the one shown in Figure A.3, the HCS asks the protection