STATENS SERUM INSTITUT

NATIONAL SUNDHEDS-IT

REFERENCE ARCHITECTURE FOR COLLECTING HEALTH DATA FROM CITIZENS

Version 1.0 (English)

National eHealth Authority

June 2013

REFERENCE ARCHITECTURE FOR

COLLECTING HEALTH DATA FROM CITIZENS

Version 1.0 (English)

National eHealth Authority

June 2013

Contents

1 Summary

This reference architecture is to act as the common reference for business areas and ICT solutions relating to the collection of health data from citizens. The National Action Plan for Dissemination of Telemedicine identified this as an area that can contribute to increasing efficiency in the healthcare sector. Therefore, the required framework has to be established for simple and cost-effective national dissemination of telemedicine solutions.

This reference architecture forms the framework for approving national standards for collecting health data from citizens and it will act across organisational boundaries and ICT systems.
This reference architecture is to support the dissemination of telemedicine solutions by ensuring a standardised and simpler way of collecting data and making it available to employees in the healthcare sector.

The focus of the reference architecture is on the data flow from the individual citizen. The data is collected from the citizen and is passed on electronically to data repositories from which health professionals across all organisations can access the data that is relevant for the individual patient's treatment. Introducing standards for how data is communicated enhances the possibility for reusing both data and ICT solutions, thereby reducing the costs associated with establishing ICT solutions.

The goal is to accelerate dissemination, as well as reduce the costs of establishing and further developing telemedicine solutions through standardising the way in which the data collected is communicated from monitoring devices and application hosting devices to WAN devices. By making data available to health professionals as entire sets of data or as 'documents' (see the reference architecture for document and image sharing), data is made available in a simple and efficient manner to all relevant parties working together for the individual citizen.

The **main recommendation** of the reference architecture is to partially base the architecture on the Continua Health Alliance Framework which profiles a number of existing standards for data communication from health monitoring devices, and partially base it on the HL7 Personal Healthcare Monitoring Report (PHMR) standard and on the IHE Patient Care Device PCD-01. The objective of this recommendation is to ensure that the reference architecture can also work in an international context.

When developing and implementing telemedicine solutions this implies firstly specifying requirements for monitoring devices and IT equipment to comply with the communication standards set out in the Continua Framework.

Secondly, it implies specifying requirements that data collected from citizens is made available to healthcare providers through the establishment of an infrastructure that enables document-based access using profiled IHE XDS standards. Finally, the reference architecture recommends that health data collection be based on the HL7 Personal Healthcare Monitoring Report (PHMR) standard for the content-related structuring of data.

The most important overall **consequence** is that a uniform way of collecting, communicating and storing citizens' data is established which makes it simpler to establish data collection, reuse existing solutions and make data available to the relevant healthcare providers.

2 Introduction

As is the case throughout the world, the Danish healthcare sector is under increasing pressure. This is due to an ageing population and a greater number of people with chronic diseases, as well as to the fact that there

are more treatment options in the healthcare sector which make it possible to treat effectively far more diseases.

At the same time, there is a need to ensure that the costs of healthcare services are kept in check. One goal is therefore to ensure that a greater number of patients can be treated without increasing costs, for example, by using telemedicine solutions in local and regional healthcare services and cross-sectoral collaboration.

The National Action Plan for Dissemination of Telemedicine(REF01) anticipates that telemedicine solutions can be used to

> *"reduce costs and to make better and more efficient use of resources at local-government and regional-government levels. The benefits in terms of financial and quality improvements from using telemedicine include having more tasks solved according to the principle of lowest efficient cost (LEON principle), coherent patient pathways across sectors, as well as reduced numbers of hospital admissions, days of admission and outpatient visits. Furthermore, telemedicine will empower patients to take part more actively in their own treatment."*

The Action Plan indicates that the premise for faster dissemination of telemedicine solutions is to standardise and ensure consensus about telemedicine, including preparing a reference architecture and standards that support the use of telemedicine solutions.

One of the areas with highest priority in relation to telemedicine is preparation of a reference architecture for collecting health data from citizens. The purpose of this reference architecture is to set a framework for Danish-profiled standards for the collection, communication and storage of data from devices in the patient's home, as well as communication
of data to the repositories from which eHealth systems can access, use and process the collected data.

In order to further develop and improve work on reference architectures, we would like to receive feedback on how the reference architecture is being used and any issues arising in this context. Comments on the reference architecture can be submitted to

soaafdelingspost@ssi.dk

2.1 What is a reference architecture?

The report "Standards and reference architectures for the eHealth area" is based on the definition from the National IT and Telecom Agency:

- *"A reference architecture is a well considered method of developing ICT solutions within a specific area.*
- *The reference architecture describes the overall logic structures and concept apparatus for the specific area such that there is a good foundation from which to work when creating cohesive ICT solutions.*
- *In addition to the logic structures and concept apparatus, the reference architecture also describes the fundamental logical business services and concepts within the focus of the reference architecture.*
- *The generic business services and concepts to be used in the interface around the reference architecture are often also described at logic level.*
- *The reference architecture can be described at several levels of abstraction. At a very high level of abstraction, only the basic structures and the adjacent surroundings are shown. At more detailed levels, logic services, core concepts and* ***interactions*** *between these are often described.*

- *A reference architecture sets common indicators and principles for development within the area. The reference architecture provides both the public authorities (orderer) and suppliers (providers) with common targets for development of the area."*(REF02)

Therefore, a reference architecture covers a limited area in which, at the highest level, business targets for the area are set and the required properties of solutions for the area are described. After this, the overall principles for solutions are established, solution elements and processes are described, and, on the basis of this, the areas which can be standardised are identified (REF03). A reference architecture can be described in greater or less detail, depending on requirements.

The figure below illustrates the correlation between reference architectures and standards.

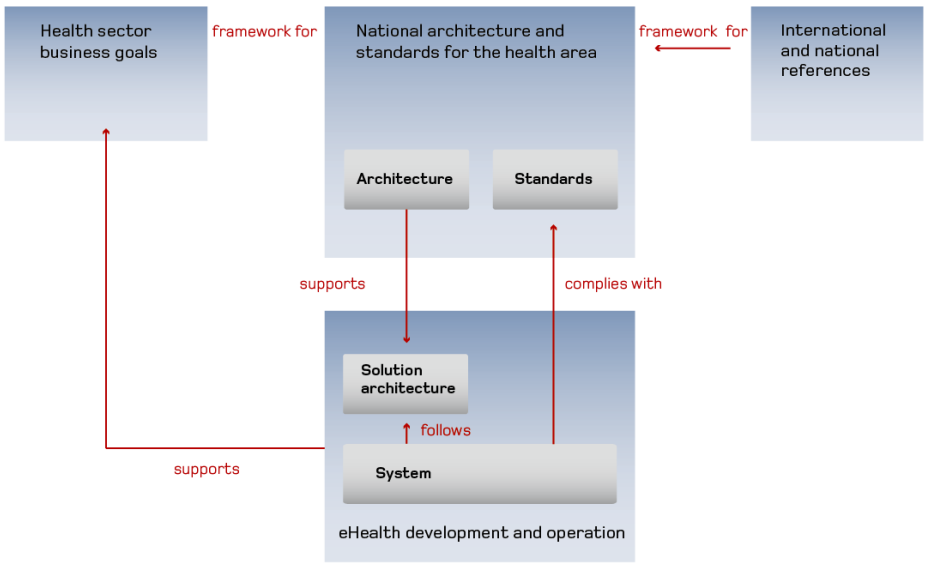


Figure 1 **Architecture and standards in the health sector**

2.2 The main content of the reference architecture

The reference architecture defines guidelines for standardised, efficient and secure transfer of measuring and monitoring results, including images, video and text messages, so that these can be made available to the health professionals that need them in treatment of patients. The data may have been collected by the individual citizens themselves or by health professionals assisting the individual citizen.

The information must be made available to the parties in a way that ensures independence between the internal structure in the systems supplying the data and the systems consuming the data.

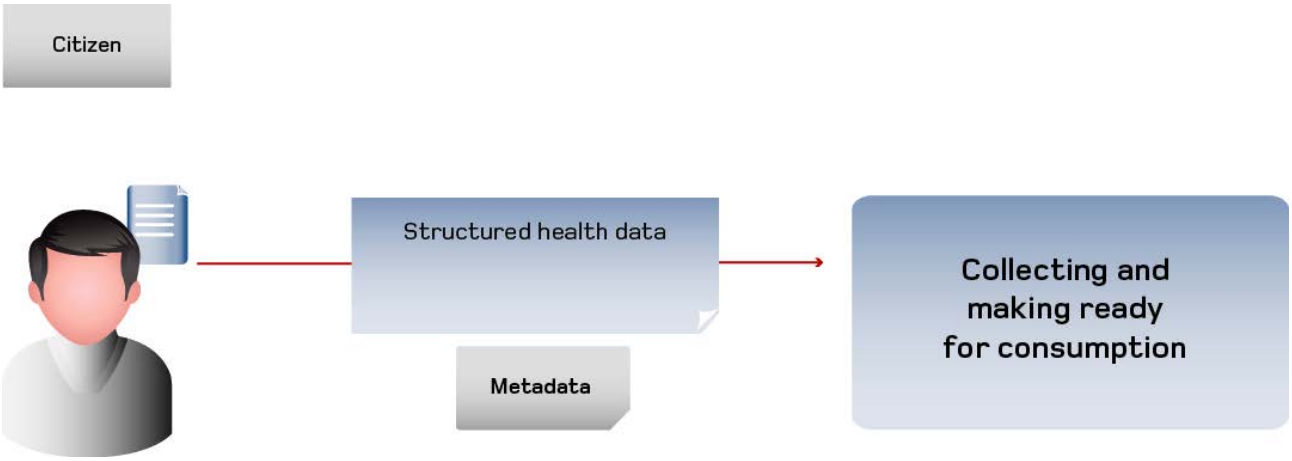


Figure 2 **Collecting health data from citizens**

Furthermore, the reference architecture is to contain proposals for technical standards and standards related to content, which facilitate the implementation and use of data collected from citizens. Where there are no existing mature international or national standards, the reference architecture should identify areas that need further development.

2.3 The central concepts of the reference architecture

The reference architecture utilises a number of concepts and terms that are vital for establishing clarity and understanding.

Some of these concepts originate from the Danish Health and Medicines Authority's database of concepts, while others have been defined in relation to this reference architecture and, therefore, apply only when using this reference architecture. The concepts of this reference architecture may subsequently be adjusted as required when a concept apparatus has been prepared for the telemedicine area.

For the purposes of this reference architecture, we have therefore chosen to operate only with the key concepts required to ensure a common understanding of the specific field of collecting data from citizens. In this context, the primary concepts are:

Monitoring device: equipment that generates various types of data about the citizen's health.

Application hosting device: An electronic unit that collects data from a monitoring device situated locally with the citizen, and which sends the data on to a WAN device.

WAN device: ICT system in which collected data is stored and prepared for consumption in an IHE repository.

Repository (IHE): The document repository is responsible for both the persistent storage of documents as well as for their registration with the appropriate document registry.

2.4 The purpose of a reference architecture for collecting health data from citizens

The reference architecture is to act as the common reference for healthcare providers when establishing telemedicine solutions that involve the collection of health data from citizens.

The purpose of the reference architecture is to ensure an architectural framework for determining standards for collecting and disseminating this data across organisational boundaries and ICT systems.

Focus is on interoperability and reuse, that is, how to ensure that the collection of health data from the individual citizen takes place appropriately, so that solutions can be reused and data can be made available for the healthcare providers that need it in connection with treatment.

2.4.1 Scope

The reference architecture for collecting health data from citizens is based on the primary consumption of data for patient treatment.

Any consumption of the collected data for secondary purposes (research, quality development) is not described.

This reference architecture only covers how health data is collected from the individual citizen and how it is made available for users of data. In other words, the reference architecture describes the flow of data from the citizen to the WAN device and from the WAN device onward to a repository from which the data can be accessed by health professionals and the citizens themselves. The reference architecture does not cover how the health professionals use the data.

Telemedicine solutions based on interactive communication between individual citizens and health professionals, e.g. videoconferencing, are not covered.

Nor does the reference architecture address the quality of monitoring devices. Those in charge of collecting data are responsible for ensuring that the devices meet the relevant quality requirements and approvals, and for ensuring that the device is being appropriately monitored, maintained and repaired/adjusted.

The quality of medical devices is covered by the EU Medical Devices Directive (REF04), see Annex A for more on this.

2.4.2 Relationship to other reference architectures

This reference architecture has a limited scope and should therefore be included in the context of other reference architectures describing adjacent areas.

Firstly, this applies to the reference architecture for document and image sharing (REF05), which sets the framework for how to make various types of information available to several providers and consumers in a standardised way that does not require prior knowledge about the internal structure of other ICT solutions. This reference architecture for collecting data from citizens does not address the display of collected data for consumption, however it describes the interface between the two reference architectures.

The use of the reference architecture for document and image sharing requires that collected data is displayed as structured documents or images with related metadata. This aspect is addressed in the following to the extent that it is relevant for understanding the reference architecture for collecting health data.

The reference architecture for information security (REF06) is a relatively generic framework which does not describe specific technology choices. In this reference architecture for collecting health data, the principles and framework for information security will be included as a part of the description of the technical architecture.

A technological reference architecture for webservices will be prepared in 2013. Once this reference architecture is available, the reference architecture for collecting health data from citizens will be adjusted.

In addition to the reference architectures prepared or planned under the National eHealth Authority, the Continua Health Alliance (in the following referred to simply as Continua) reference architecture (REF07) will be incorporated, where relevant in relation to this reference architecture. Continua can be understood as a technical framework/reference architecture for collecting monitoring data. Continua is not a standardisation body, but it uses existing standards and places these in a coherent use-oriented context.

The scope of the reference architecture for collecting health data also covers the local-government level and correspondence should therefore be ensured with Local Government Denmark's reference architecture (REF08), which is a framework architecture for local-government ICT solutions. The purpose of this framework architecture is to improve local-government digitalisation efforts generally and to ensure a foundation for competitive tendering of existing ICT solutions.

The correlation between the reference architectures mentioned above is given in the figure below. As is evident from the figure, there are various types of reference architecture. Basic reference architectures such as the reference architecture for information security apply generally, whereas the reference architectures become more specific toward the bottom of the pyramid.

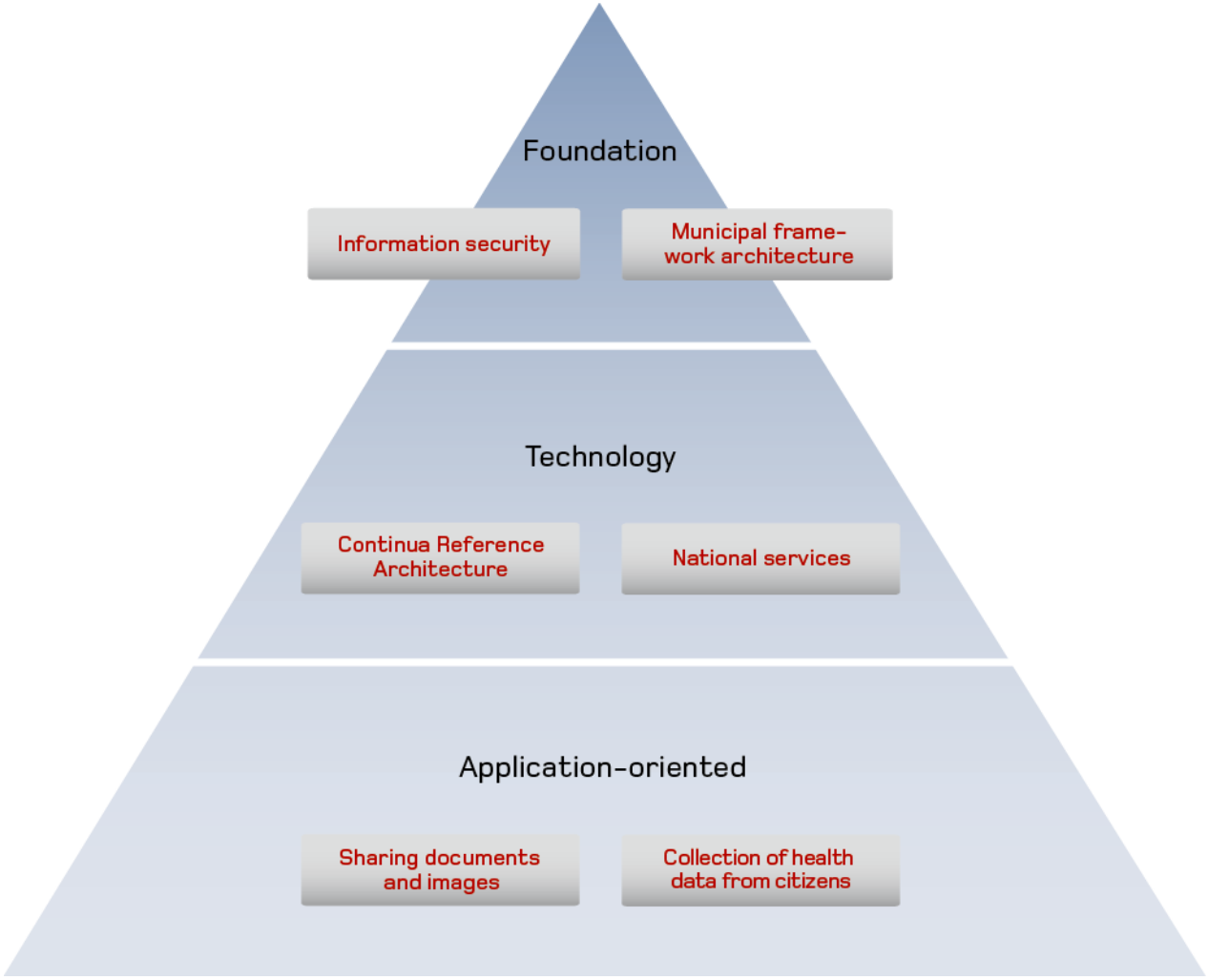


Figure 3 **Types of reference architecture with relevance for health data collection**

2.5 Use

The reference architecture is to be used in connection with requirements specification for telemedicine solutions and to establish agreements with suppliers of telemedicine equipment and related ICT solutions.

The reference architecture makes up the general framework for telemedicine solutions involving health data collection from citizens.

National profiles may have to be established for the standards recommended by the reference architecture[1].

The standards have to be tested and subsequently approved separately by the National eHealth Authority's advisory committee concerning standards and architecture, before the National eHealth Authority can determine their recommendability and publish them in the catalogue of eHealth standards. In this connection, how to ensure implementation of the standards will be assessed, including whether there should be requirements for certification.

[1] Framework standards, as described in e.g. HL7, are very extensive and therefore it is important to specify which parts of a given framework standard apply to the area in question.

If the reference architecture is not consistent with other reference architectures, standards or project needs, the National eHealth Authority will enter into dialogue with the parties so that the necessary assessments and choices to establish consistency can be made collaboratively.

2.6 Target group

This reference architecture is aimed primarily at decision takers in the healthcare sector who need to decide on the instigation and development of telemedicine solutions that involve the collection of health data from citizens.

This extends to the Ministry of Health and its agencies, regional and local governments, the general practice sector, Danish Regions with RSI, Local Government Denmark, Kombit, the e-Health Portal sundhed.dk, and MedCom.

In addition the reference architecture is relevant for project managers, IT architects and developers at public authorities as well as suppliers tasked with specifying requirements and designing telemedicine solutions that involve the collection of health data from citizens.

2.7 Reader guidelines

Chapter 3 describes the strategic framework for the reference architecture and is relevant for both decision takers and solution architects/developers.

The following chapters provide more detail on the business architecture (chapter 4) and the technical architecture (chapter 5) and are primarily intended for project managers, solution architects and developers.

2.8 Development process

This report has been prepared by the National eHealth Authority in collaboration with a number of partners from the health sector and suppliers of ICT solutions to the healthcare sector.

The work group held five workshops in the period from September 2012 to February 2013. The work group included:

Peter Falkenberg, Local Government Denmark

Mette Brøsted Nielsen, Esbjerg Municipality

Irene Sandager, Esbjerg Municipality

Lars Simesen, Central Denmark Region

Allan Hansen, Central Denmark Region

Dennis Mølkær Jensen, North Denmark Region

Jan Petersen, MedCom

Henning Povlsen, Logica

Christian Graversen, DI ITEK

Svend Vitting Andersen, Pallas Informatik

Brian Hedegaard, DELTA

Sine Jensen, Danish Consumer Council

Anette Højrup, Danish Consumer Council

Camilla Wiberg Danielsen, National eHealth Authority

Thor Schliemann, National eHealth Authority

Esben Dalsgaard, National eHealth Authority

Pia Jespersen, National eHealth Authority (chairperson)

Kurt Hansen from Strand & Donslund assisted as a consultant in connection with the preparation of the reference architecture.

3 Strategy architecture

3.1 As is (the current situation)

The substantial strain on Danish healthcare services has brought about increased interest in testing telemedicine solutions that allow for the monitoring and treatment of patients in their own homes, thus reducing costs, particularly of hospital treatment.

In recent years, several pilot projects have been completed or commenced which test telemedicine solutions and which have provided the various healthcare providers with greater knowledge about the possibilities for using telemedicine.

However, many of the projects have been established as single, independent projects that have not been linked to the overall use of eHealth. Each project has ended up with its own solutions and architectures and has applied different technologies.

The fact that the various solutions do not 'speak the same language' (i.e. that the semantic content has been perceived differently) has obstructed the dissemination of solutions.

Figure 4 Individual solutions for health data collection

Figure 4 illustrates a situation in which the collection and storage of data is carried out by several health professionals, each with their own device and solution. For individual citizens, this can imply that the various measurements performed are collected by different monitoring devices and application hosting devices, which have to be installed in the patient's home or similar, and which the patient has to be able to manage.

The monitoring data is collected in a separate database with its own software application and if there are several different solutions for collecting health data, health professionals have to access the various solutions, as well as their own records systems, for an overall picture of the patient's condition.

Moreover, if monitoring results are not standardised, this can also make it difficult for health professionals to use the collected data; for example, if there is no agreement about which data to register or how to classify data.

3.2 Trends

3.2.1 Business trends

The many projects that have tested, or are in the processes of testing, different telemedicine technologies have generated important experience about how to achieve a greater effect by involving the citizen and his or her surroundings in monitoring their health and in treating their diseases. With a view to ensuring greater dissemination throughout the healthcare sector, a more standardised market for devices and ICT solutions for data collection will have to be established. Intensive work to achieve this is taking place under e.g. the IEEE[2].

[2] The Institute of Electrical and Electronics Engineers, Inc., which is an international non-profit organisation for the advancement of technology.

Some of the larger telemedicine projects, e.g. the projects under the national action plan, are working with solutions that can manage several diseases, even in the same patient, so that the diseases can be understood in context. These projects therefore also work on integrating the collected health data in the ICT solutions of health professionals, for example the electronic health record (EHR) and the electronic care record (ECR), and medical practice systems, so that the collected data are widely available and can be included with other relevant health information when assessing the condition and treatment needs of patients.

This is also the background for the National Action Plan for Dissemination of Telemedicine. The parties behind this action plan have identified a number of areas that are to provide support for more coherent and standardised development of telemedicine solutions and thus ensure a balance between outcomes and the resources invested.

This is also reflected in the strategy work on telemedicine at both local-government and regional levels, an important element of which is a desire for standardised solutions that can be used (and reused) across the healthcare sector.

3.2.2 Technological trends

This section describes some of the technological trends of relevance for the reference architecture. The trends described express the future developments expected by suppliers and consumers of telemedicine solutions. In the table of trends, note in particular the paragraphs describing the consequences for the reference architecture.

Below is a description of the selected technological trends and a brief review of the most important consequences for the reference architecture.

Technological trend	Description and consequence
Medical devices and consumer products	Manufacturers of monitoring devices to measure and monitor health data are currently shifting their attention to the consumer market. Large-scale procurements are relatively stagnant within the health sector, so the shift of market focus should be seen in a sales perspective in relation to the importance of revenue-earning opportunities for manufacturers. The consumer market is currently the primary driver of technological development. This applies to monitoring devices as well as to software applications. A number of US manufacturers are excluding the medical requirements for the devices and are omitting to obtain approval from the Food and Drug Administration. There is also a tendency to manufacture existing medical monitoring devices in simplified versions targeted at the consumer market. In the short term, this means growth for the manufacturers of medical monitoring devices, but it also creates a market which will lack transparency about the products on offer until the market has found its bearings. There will be competition for market share and there will be many proprietary solutions. In the long term, what we today know as medical devices will

Technological trend	Description and consequence
	become part of our everyday lives, for example integrated into our wrist watch, mobile phone, or as a part of our diet. This does not change the fact that the statutory requirements still have to be met for medical devices. **Consequences** • The same monitoring device can be procured in both a medical and a consumer version. There should be requirements for certification of the device's communication, in order to guarantee compliance with standards and interfaces. • It is likely that certain types of monitoring device will be available only as consumer products, and that they will therefore not be suited in a telemedicine context. • With regard to certification etc., the many different types of device and equipment that will have to be managed may pose a challenge. • The reference architecture can either dictate (e.g. with regard to standards, quality, user interface/connection etc.), or it can be open and merely account for the core of the elements required to support the aim of the reference architecture
The price and size of monitoring devices	The technological development for monitoring devices follows Moore's law, which means they will grow smaller and cheaper by a factor of 2 every 18 months. There is an anticipation that monitoring devices will therefore grow ever smaller and cheaper, and that they could eventually be made available free of charge, because the devices can be included in business models which create value through collected data, activities to create data, and related commercial areas. The price of monitoring devices is expected to drop, and, in future, citizens may procure the devices themselves, e.g. on the advice of a health professional. In the long term, medical devices will be built into things we already surround ourselves with. There will be no need to buy separate medical devices, as these will already be integrated into things that we wear or use on a daily basis. The devices will probably continue to be simple devices performing simple tasks, such as monitoring your weight or pulse, or similar measurements that can be used for multiple purposes. Our surroundings will be more 'intelligent'. This applies to things close to our body, such as our clothes, shoes, jewels and similar, as well as our home, our car or similar which will be able to perform measurements, receive and communicate measurements, and react to trends in the data measured.

Technological trend	Description and consequence
	Consequences • Interfaces for submitting monitoring data to a WAN device must be well defined and based on standards profiled as globally as possible. • As a consequence of this monitoring devices might be manufactured that can actually replace e.g. expensive analysis equipment (REF09). • Looking further into the future, the monitoring device will already be with the citizen when a measurement needs to be commenced. In future, the reference architecture should therefore enable activation of the monitoring device and collection of monitoring data.
Usability and requirements for competences in the consumer	In upcoming years, devices are likely to place requirements on other equipment used and on the citizen's ability to connect and apply the monitoring device. This could even go so far as to prevent certain sections of the population from using the system. In terms of use, most solutions are currently independent solutions, each targeted at its own target group with certain competences. It is expected that a great number of devices will be produced by manufacturers that already supply equipment to hospitals. Consequently, these devices may require specialist (care- and medico-technical) insight. These devices will reflect a greater emphasis on the needs of health professionals than on usability and the needs of the actual end-user, i.e. the citizen. This issue is being addressed legislatively, with a view to ensuring that products have better usability. **Consequences** • As the users of the monitoring devices are citizens, the devices must be designed so that citizens are able to operate and configure them themselves. • For more complex devices, it may be difficult to ensure a degree of usability so that all citizens are able to operate the device. There will be greater demands on the competences of citizens and there may be a need to provide professional support to some citizens in the use of the device.
Mobility	Mobility trends cover both monitoring devices and application hosting devices. The trend is that both are becoming more mobile, and products that do not support mobility will become irrelevant or will disappear from the market within only a few years. • In principle, the reference architecture is indifferent towards mobility, and it can accommodate solutions that

Technological trend	Description and consequence
	support both mobile and stationary devices. • Continua is currently working on a mobile framework architecture which will subsequently be incorporated in an updated version of this framework architecture.
Personal or shared devices with the citizen	The development is towards the individual, as more and more functionalities are being integrated in smartphones and other mobile units, e.g. tablets, which are generally personal. It is likely there will be still be a demand for other types of unit. **Consequences** If the monitoring device is responsible for identifying the person on which it is performing the measurement, application hosting devices should be shareable between several persons.
Integration of the monitoring device and the application hosting device	There is a tendency to integrate mobile devices and application hosting devices in single integrated units.
Better personal identification	Biometry has not yet been integrated in monitoring devices and application hosting devices. Certain personal health record solutions have a pattern recognition functionality so that they can deduce with fair certainty from the selected data which individual the data was measured from.
Interoperability of units and devices	With regard to the interoperability of personal monitoring devices and application hosting devices, the industry has observed at least three trends: *Continua Health Alliance* - is the preferred route of many with regard to communication of data from monitoring devices to the WAN device. There is a need to improve the quality of data and data structures, and the IEEE and Continua are therefore in the process of defining a minimum information structure (metadata) which each unit must supply. *Microsoft HealthVault* - Sweden, and the UK, in particular, are experiencing large interest and certain suppliers are considering taking this route. HealthVault has an innate weakness because it is a proprietary solution which means that Microsoft alone defines its exchange structures. MS HealthVault certifies devices in the same way as Continua. *Proprietary solutions* - Certain manufacturers choose their own routes and build entire organisations for production, installation, monitoring, training, call centres, etc, for data collection from citizens' homes. There is great uncertainty as to whether devices from these manufacturers can be used

Technological trend	Description and consequence
	with devices and equipment from other manufacturers. **Consequences** • The reference architecture must focus on clear and unambiguous interfaces and it must ensure that chosen standards have as broad a backing as possible. • Proprietary solutions give challenges with regards to formats, interfaces and security. The reference architecture should stress that interfaces must be standardised and that any proprietary solutions must be embedded in interfaces. However, the respective market spread of Continua and proprietary monitoring devices (based on e.g. HealthVault) should be monitored continuously.
Standardisation and application of standards	We will see a greater use of standards in the medical area in the future, because the industry has an interest in promoting coexistence and interoperability (see above). Continua and IHE are good examples of the use, including the collective use, of standards. The consumer market is experiencing a gradual standardisation toward market standards driven by supplier collaboration, e.g. Continua Health Alliance. **Consequences** • To the widest possible extent, the reference architecture should recommend the use of international standards and standards applied by the market. • Danish stakeholders should attempt to influence standardisation in areas in which the reference architecture identifies a lack of standards or too much focus on national profiles.

3.3 Vision

The National Strategy for Digitalisation of the Danish Healthcare Service 2008-2012 (REF10) emphasised that citizens and patients should be included to a greater extent in their own treatment, and that knowledge and information possessed by citizens and patients should be applied actively in disease prevention and treatment.

Furthermore, digitalisation should provide opportunity for the individual to influence and take an active part in his or her own health, e.g. through shared care solutions, monitoring and home care, etc.

The National Action plan for Dissemination of Telemedicine (REF01) followed up on this Strategy and described specific initiatives to ensure that more patients can be treated using fewer resources and without compromising quality of care.

Telemedicine solutions can improve the quality of life for citizens and allow them to feel safer in their own home as they learn more about their disease and are empowered to take active part in its treatment and in preventing its deterioration. Moreover, telemedicine solutions can help improve services to citizens, for example through eliminating transport time and waiting time in connection with examinations, or through making it possible for citizens to make greater use of the freedom of choice between providers because they are less dependent on the geographical proximity of the place of treatment.

The local-government and regional levels are also working strategically with telemedicine as a tool to maintain the level of quality in services while reducing the strain on resources.

The regional telemedicine strategy (REF11) states e.g. that

> *"Telemedicine is to strengthen the Danish healthcare service by ensuring coherent patient pathways through enhanced accessibility, quality, and efficient prioritisation of healthcare services and resources."*

The strategy identifies videoconferencing, image exchange, and home monitoring as the most important focus areas, and emphasises a need for more standardisation and reuse of ICT solutions across sectors and providers.

All healthcare providers consider the collection of health data from citizens a key parameter in making treatment more efficient in connection with chronic diseases, without compromising quality of care.

Over time, the collection of health data directly from citizens could become a parameter in other treatment scenarios as well, in which both local government and hospitals use health data collection in their healthcare services. Therefore, efforts need to be coordinated to allow for the widest possible use of monitoring devices and application hosting devices for multiple purposes. Efforts also need to be coordinated to avoid inappropriately large costs of providing service and support to users.

In this context, the vision of the reference architecture is to ensure that

Health data collected from citizens may be included in the assessment of the individual's health and treatment in the same way as health data generated within the healthcare sector proper.

The reference architecture and recommended standards ensure that collection and communication of data on citizens can be performed in a simple and efficient way that facilitates quality and efficiency of services from healthcare providers.

3.4 Business goals

While the vision describes the long-term and overall goals for the area, the business goals describe the anticipated achievements within a time frame of three to five years.

It is not anticipated that all technical, organisational or semantic barriers for sharing information across the healthcare sector can be addressed within this time frame. The business goals therefore primarily cover those areas which are absolutely crucial to commencing standardisation within the area.

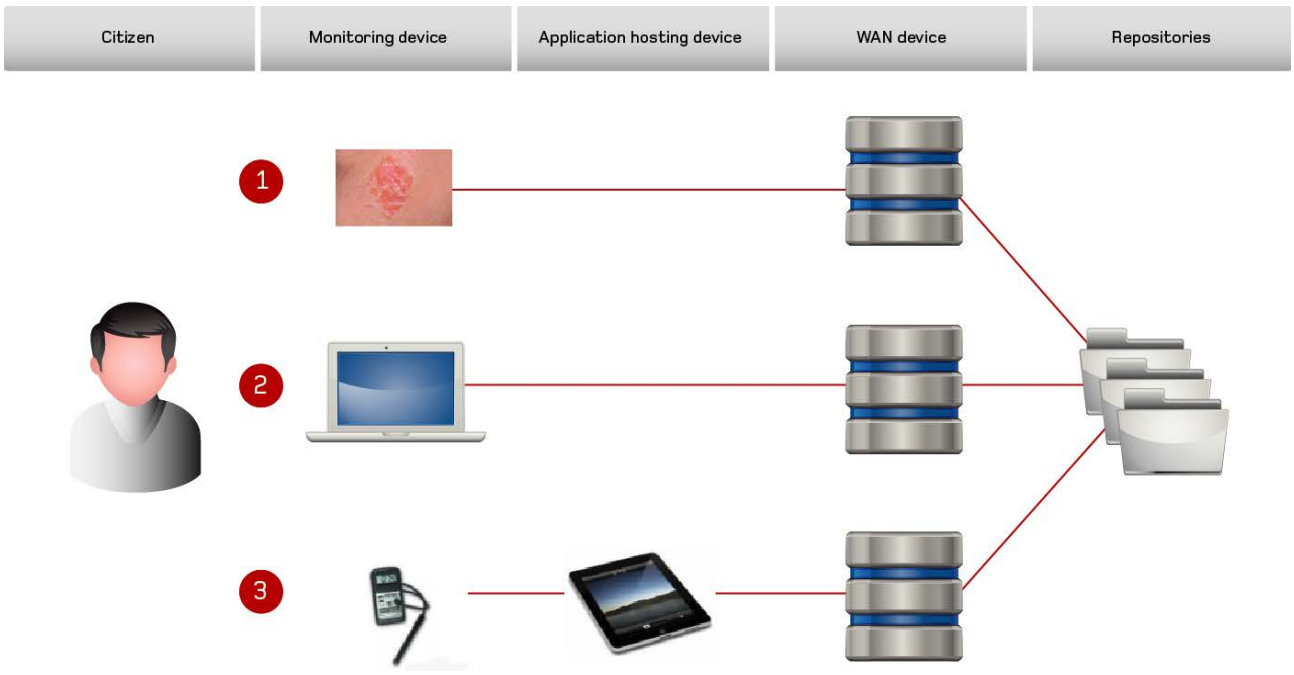


Figure 5 **Types of health data collected**

As can be seen from figure 5, various types of data from citizens are collected in different ways. The unit that communicates data is only illustrated as a application hosting device for monitoring data, but if this unit is in the form of an iPad/tablet or smartphone, it will also be possible to manually enter text messages/notes to the monitoring data.

One of the most important objectives of the reference architecture is therefore to **set out the framework for determining standards for collection and communication of health data from citizens.** This includes technical standards aimed at making it easier and less costly to integrate decentralised monitoring devices and application hosting devices into the ICT solutions of health professionals, as well as content-related standards and classifications that address the need for semantic interoperability in the healthcare sector. Another important element is to define a framework for how to coordinate efforts aimed at citizens, in particular in situations involving data collection from several types of monitoring devices, or in situations when there is a need to be able to use the same data across several healthcare providers.

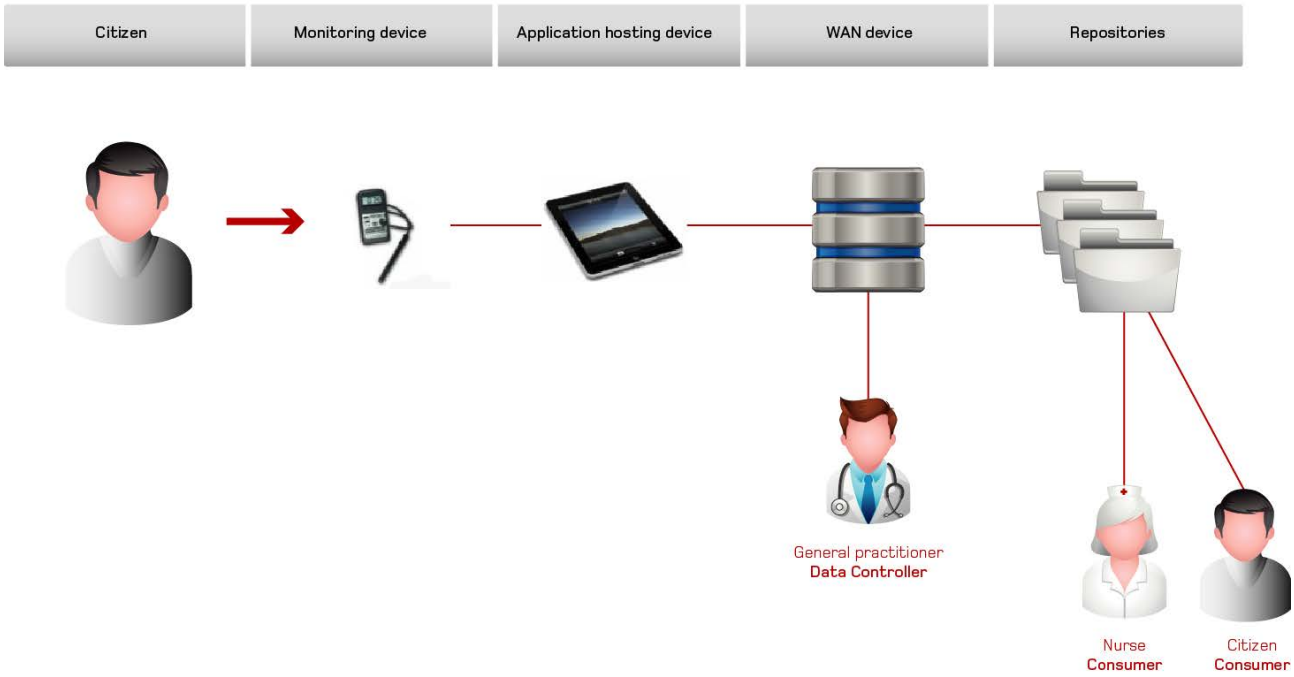


Figure 6 **Several health professionals using the same monitoring device**

Figure 6 illustrates a situation in which the same type of monitoring device is used by several people, for example, when the general practitioner and the local elderly care service make use of the data collected from the same monitoring device. The general practitioner initiates the monitoring and is therefore responsible for the device and for data control in relation to data collection. The other user, i.e. the nurse in the local elderly care service, accesses the collected data through the repositories in which it is stored. From here, also the citizen can access his or her collected data in context with other health information that may have been collected and recorded about his or her treatments by other healthcare providers.

This scenario requires that the providers using the same monitoring device agree on the scope of data collection. As a general rule, the owners of the system will be responsible for data collection and for entering into agreements with the other users about which data will be made available for use.

If the citizen has several types of monitoring device, it may be relevant to consider the possibility of using the same application hosting device for all of these devices. In this situation, illustrated in the figure below, the different users would each have to install their own application in the application hosting device and they would each be data controller for their own part of the data collection. This scenario requires that the healthcare providers enter into an agreement about who is responsible for the application hosting device as such, and they need to ensure that the two types of data collection can take place unhindered over the same network connections. In this situation, there will have to be a clear agreement as to who is responsible for the hardware and the network connections.

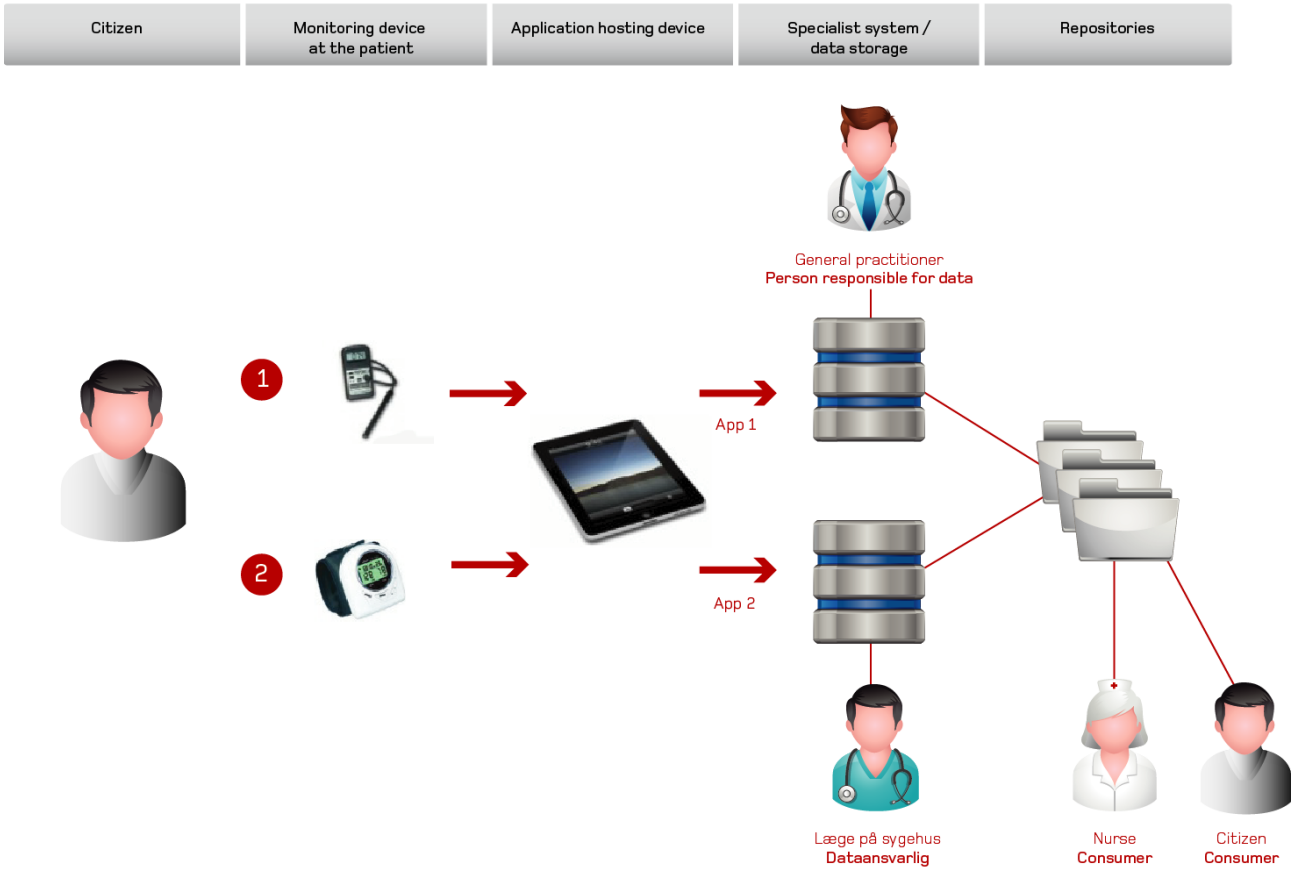


Figure 7 **Several health professionals sharing the same application hosting device**

Therefore, it is important that the reference architecture contributes to clarifying the general principles for ownership and data control in relation to the data collected, with a view to creating clarity about roles and responsibilities, including the responsibility for drawing up an agreement with the citizen, for ensuring the quality of the data collected, for providing support to the citizen, for the communication equipment, etc.

3.5 Value creation from the reference architecture

The reference architecture for collecting health data from citizens is to set the framework for how to procure, implement and operate solutions that collect health data from medical devices or directly from citizens.

In future, citizens will have to play an active role in their own treatment, and ICT solutions therefore have to be developed which can be used outside the healthcare sector's normal settings, namely in the home or at the current location of the individual citizen. A secure and efficient way has to be ensured for submitting the data to the data storages (WAN devices) an onward to the repositories, and the repositories must be accessible from the ICT solutions used by health professionals or by the citizen via sundhed.dk.

The table below is a summary of the intended benefits from the reference architecture for collection of health data from citizens.

Outcome	Benefits

Common concepts	The reference architecture establishes a common conceptual framework concerning the collection of health data from citizens, which makes it easier to communicate and ensure competitive tendering of solutions.
Easier decisions on tendering and procurement Greater maturity of projects	When using competitive tendering, the conditions for tendering are known by and are the same for all suppliers
A common reference architecture	Simplifies the task of specifying requirements for individual and interlinked solutions
Common supplier requirements	Greater possibility for influencing suppliers' products Simplifies the tender-making process for suppliers
Enhanced market potential Export of telemedicine solutions	Coordination between national and international standards
Description of domains and relationship between stakeholders in the reference architecture	Clear division of responsibilities
Enhanced efficiency	The reference architecture and associated standards ensure the framework allowing citizens to collect and report health data on their own or through the help of a health professional. Automatic transferral of collected health data in a standardised way will reduce resource consumption in the healthcare sector, and resource consumption for transport to and from examination and consultation visits. [3]
Mobile citizens	The use of international standards in the integration of monitoring devices will increase mobility for citizens, inside as well as across national borders, and will ensure greater flexibility because it will be easier to replace equipment.
Guidelines for procurement of monitoring devices	The recommendations and recommended standards from the reference architecture will serve as guidelines for healthcare providers and citizens buying monitoring devices.

4 Business architecture

4.1 Principles

This section reviews the principles of the architecture forming the basis for the design of the reference architecture. The basis for selecting principles originates mostly from the architecture principles adopted for the health sector (REF12) but where relevant it also draws on common public sector architecture principles.

[3] The National Action Plan for Dissemination of Telemedicine describes the anticipated size of staff and financial savings to be harnessed from nationwide deployment of telemedicine solutions (REF01)

The following includes only principles aimed specifically at health data collection from citizens.

Business principles
Clear division of responsibilities
Health data is made available to all healthcare providers as required
Selection of standards guided by what is widely supported by the market (now and in the future)
Support use of international and national standards
Information principles
Standardisation of metadata is a national task
Collection of health data at an appropriately secure level
Technical principles
Use of national infrastructure

4.1.1 Business principles

Title	**Clear division of responsibilities**
Description	In order to benefit from telemedicine solutions, it should be possible to determine precisely who is responsible for correct functioning and use of devices etc.
Rationale	Health data collection from citizens involves moving outside the normal healthcare sector organisation, and health professionals from several providers will often be involved in the delivery of the task in question. Who is responsible for what is not always clearly defined.
Implications	The reference architecture should be designed so that it allows for the clear division of responsibility for the device's function, data, security, support and communication channels.
References (REF12)	

Title	**Health data is made available to all healthcare providers as required**
Description	Health data is collected from the citizen and placed in a single common repository or in several repositories with possibility of transparent searches between domains, so that health professionals

	with a treatment relationship to the citizen can access relevant data in a simple and uniform way. Communication between domains takes places in a standardised way.
Rationale	Data exists independently of the source systems that generated it and access to data is independent of the specific ICT solutions in which the data is stored.
Implications	It is a requirement that telemedicine solutions involving health data collection from citizens, and which are to be used across healthcare providers, are integrated into the shared national infrastructure.
References	

Title	**Selection of standards guided by what is widely supported by the market (now and in the future)**
Description	The reference architecture should contain the basis for how to identify the standards to be used in connection with collection and communication of health data from citizens.
Rationale	The reference architecture should point to the standards which can contribute to ensuring broad market support, including in the longer term, and thereby increase the rate of dissemination of solutions that involve the collection of health data from citizens.
Implications	The standards which are recommended for use in connection with collecting and communicating health data are to be reviewed by the advisory committee for architecture and standards and subsequently published in the catalogue of standards for the health area.
References	

Title	**Support use of international and national standards**
Description	This is a general architecture principle which, for this reference architecture, means that it should also point to any standards which can contribute to increasing dissemination and rate of dissemination of solutions for collecting and communicating health data from citizens.
Rationale	The use of international and national standards ensures that it is possible to communicate with providers within other sectors in Denmark and with providers abroad. At the same time, the use of international and national standards ensures a broader range of suppliers and it ensures that Danish suppliers using these standards can expand the market for their solutions.

Implications	It needs to be assessed whether Continua's framework will be able to support the objective of the reference architecture. Profiling existing (mature) standards requires consensus between the parties who are to implement the standards. The implementation of international standards will lead to a need to be able to influence how the standards are set, in order to ensure that standards used in Denmark comply with international standards; also in the future.
References	Overall architecture principle F2: International, national and local initiatives are to be coordinated with a view to reusing both new and established solution elements, standards and infrastructure. The common public sector reference model (FORM).

4.1.2 Information principles

gTitle	**Standardisation of metadata is a national task**
Description	To underpin cross-sectoral use of data, a model is to be made for use of metadata to search and classify data.
Rationale	The metadata to be used for searching should be standardised within the individual domain and across domains, if it is to be possible to manage transparent searches across indexes.
Implications	A standard owner is to be appointed to be responsible for development and maintenance of common metadata.
References	Overall architecture principle I2: Real cohesion via information sharing requires establishment of semantic interoperability in relevant areas, taking into account the desired utility value. Reference architecture for document and image sharing IHE

Title	**Collection and management of health data at an appropriately secure level**
Description	Collection, communication and storage of personal identifiable information should be in accordance with requirements in the Danish Health Act and the Act on Processing of Personal Data.
Rationale	It must be ensured that data is accessible, up-to-date and correct and that unauthorised persons cannot gain access, inadvertently or intentionally, to sensitive information.
Implications	If health data is stored for longer periods of time in the application hosting device, the device should comply with the requirements of

	the Danish Statutory Order on Security (REF13). The communication of health data must be secured, for example using encryption or dedicated connections. In connection with access to collected data, security solutions should be established which support authentication and authorisation of users and validate that there is an existing treatment relationship. Traceability should be supported using logging in all places where this is relevant.
References	Overall architecture principle I1: For information sharing, clear definition of data ownership (data responsibility), maintenance responsibilities and usage policies must be set. Overall architecture principle T1: Security related to cross-sector workflows must be supported by the national infrastructure. Reference architecture for information security

4.1.3 Technical principles

Title	**Use of national infrastructure**
Description	The reference architecture for collecting health data from citizens is based on the use of the shared national infrastructure.
Rationale	Health data collection should be able to act as an integrated part of the national infrastructure and ensure reuse of solutions.
Implications	The reference architecture should incorporate use of the national infrastructure and security infrastructure in describing frameworks and use of standards.
References	Overall architecture principle T1: Security related to cross-cutting workflows must be supported by the national infrastructure. Reference architecture for information security. Reference architecture for sharing documents and images.

4.2 Concepts

There is currently no overall concept model concerning telemedicine and this document therefore only defines the concepts required to understand the reference architecture.

This document will therefore have to be reviewed when an overall concept model for telemedicine has been prepared at a later stage.

Information (concept, term, synonym)	• Description
• **Data**	• observation that can be concluded from • Comment: • Data is represented in the outer world, i.e. outside the mind, by formalised signs and symbols, such as figures and letters.
• **Treatment**	• intervention, the health purpose of which is to affect the patient's health • Comment: • For example, prevention, diagnosis, examination, treatment, care and rehabilitation/training.
• **Monitoring device**	• Equipment that generates data about the citizen's health status.
• **Application hosting device**	• An electronic unit that collects data from a monitoring device situated locally with the citizen, and which sends the data on to a WAN device.
• **WAN device**	• ICT system in which collected data is stored and prepared for consumption in an IHE repository. • Comment: The nature of this preparation depends on the purpose of the data collection but, as a minimum, it ensures that unique personal identification and other relevant metadata has been added.
• **Metadata**	• Data which defines and describes other data (ISO/IEC 1179-4:2004(en)) • Comment: • Structured information used to describe, administrate and retrieve data (http://digitalbevaring.dk/metadata/)
• **(Document) Repository (IHE):**	• The physical location at which documents and images are stored after creation and from which they can be retrieved for subsequent consumption.
• **User of an IHE repository**	• A user who accesses an IHE repository in order to search and retrieve relevant documents.
• **System owner**	• Owner of an information asset who has the rights to, and responsibility for, an information system. • Comment: • The organisation responsible for the hardware and/or software

	used for data collection. The system owner and data controller can belong to the same organisation.
• **Data controller**	• Person who, alone or with others, decides for what purpose, and with which tools, information may be processed.

4.3 The business processes related to collecting health data from citizens

The specific business processes linked to health data collection, and for which there is a need for support from ICT solutions, are as follows:

- Collaboration agreements
    - Potentially, many parties will be involved in health data collection from citizens, and agreements have to be drawn up between these parties to clarify the segregation of responsibilities and tasks, and identify what the various parties can expect from the collaboration. Agreements may be between the system owner and citizens, between the system owner and other data consumers, between the system owner and the data controller and possibly suppliers.
- Installation/setup of monitoring devices and communication devices
    - Monitoring devices and communication devices must be installed at the citizen's home etc. and the citizens (and possibly health professionals) who are to take part in data collection must be instructed in how to use the devices, including how to deal with any faults.
- Health data collection
    - Health data collection should take account of the specific data to be collected and sent on to the WAN device, at what time intervals data collection is to be made, and the standards (classifications) the data collected is to comply with.
- (Manual) input of supplementary information
    - In some cases there may be a need to supplement or adapt the data collected. For example, if data has been collected with a non-personal identification mechanism, the WAN device will have to couple the data to the person to whom it relates. This could be automatic, but there may also have to be a health assessment and processing of the data before it is displayed for other consumers in the healthcare services.
- Metadata to search for collected health data
    - The metadata which is to enable search and retrieval of relevant data across the healthcare services is added to the collected data in the WAN device at the latest.

4.4 Services / business services

The reference architecture describes a set of business services and technical services to be supported and implemented by solutions which realise all or parts of the described reference architecture. In addition to the business services, there is a description of a set of more technical services prepared on the basis of the Continua use-case descriptions (REF14), as these cover data collection. This ensures consistency between the services and the system-technical target image.

Business services focus on services around data collection, as consumption-related services have been described in the Reference Architecture for document and image sharing [REF 4].

Business services

Business service	Description
Monitoring and collecting data	Services which support the citizen in monitoring/measuring health and collecting the associated monitoring data via monitoring devices.
Collection of other health data	Services which support collection of other health data which is not monitoring data.
Health data enrichment	Means that monitoring data can be enriched, e.g. with further metadata.
Determination of patient identity	Helps couple a measurement (collected monitoring data) with a citizen's patientID so that monitoring data can be displayed and consumed by healthcare staff.
Data transfer	Services which support data transfer from monitoring devices to the application hosting device and onwards to the WAN device.

Technical services

In order to ensure traceability to Continua use cases, the original terms are used.

Technical service (Continua Use case)	Description
Controlled Data Sharing (consent management)	Services include interchange of declarations of consent to consume monitoring data, including securing privacy through encryption services.
Information reliability and authenticity (integrity)	Services which ensure that only documents passing a signature check are accepted.
Patient Identity Mapping	Services which map between local ID and ID used in data exchange or data storage.
WAN Controlled Data Sharing	Services which support exchange/transfer of messages with monitoring data over a Wide Area Network (WAN).
Low Power LAN	Services which support integration of monitoring devices with limited processing power and low energy capacity in a Continua-based architecture.
Low power LAN: ZigBee	Services based on the ZigBee Health Care profile version 1.0.

	Provide wireless transfer of data from monitoring devices to the application hosting device.
Extension to One-to-Many Connectivity	Services which support establishment of simultaneous connection between a monitoring device and several application hosting devices.
Bluetooth LE Blood Pressure Monitor and Bluetooth LE Heart Rate Monitor	Services which offer transfer of monitoring data from monitoring devices to a application hosting device using low-energy Bluetooth.
Peak Flow Device	Services which offer both PAN and LAN transfer for data from Peak Flow devices.
Body Composition Analyzer	Services which offer monitoring data relating to body composition4 over Bluetooth, ZigBee or a wireless network.
Glucose meter	Services which offer both PAN and LAN transfer for data from blood glucose meters.

With regard to images, it will be relevant to assess the need for general business services in relation to the project to disseminate the use of telemedical ulcer assessment(REF15).

5 Technical architecture

5.1 System-technical target image

This section describes the system-technical goals for the reference architecture for collecting health data from citizens which make it possible to support the vision and business goals described above.

As part of the system-technical target image, the technological trends and current ICT situation is described for areas with a direct influence on the reference architecture or which cover aspects the reference architecture must take into account.

5.1.1 AS-IS ICT architecture

5.1.1.1 Continua Framework

A significant part of the reference architecture is based on the Continua Framework and therefore Continua is deemed to be part of the AS-IS situation.

The Continua Framework is developed and maintained by Continua (REF16), which is an open, non-profit industrial alliance composed of a broad cross-section of medical and technological enterprises; working together to improve the quality of personal healthcare.

The Continua Framework is illustrated in the figure below, and it describes the use, composition and profiling of a number of standards which together make up a consistent foundation for collecting and

[4] Body Composition Analysis is an advanced fat percentage measurement which, in addition to fat percentage and a number of other measurements, also shows your "metabolic age" which is an indication of your state of health and your risk of developing cardio-vascular diseases.

exchanging health data measured via various monitoring devices and application hosting devices, and which ensure interoperability between devices and components. The Continua Framework applies to monitoring devices and application hosting devices to deliver data in electronic health records or personal health summaries.

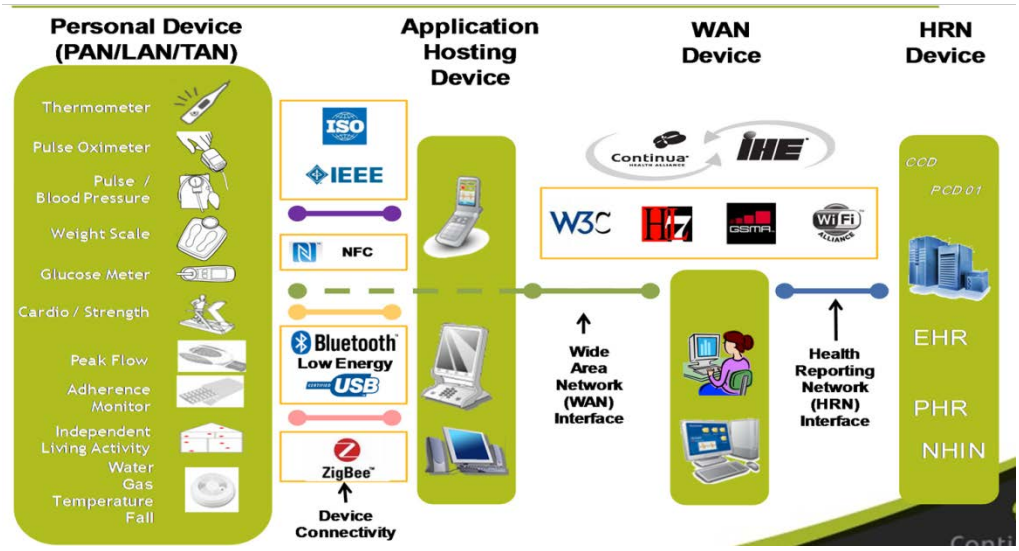


Figure 8 **Continua Framework**

The Continua Framework also includes the option for suppliers to obtain certification and an interoperability test of their devices and components. Certification includes a compliance test for the relevant interfaces for the device.

5.1.1.2 Pilot projects

A number of projects are being run under the National Action Plan for Dissemination of Telemedicine, which are relevant for the areas covered by the reference architecture. These projects and the experience acquired from them have contributed to the design of the system-technical target image.

The projects are primarily the three described below, where data collection from citizens has been part of the project.

- KIH-Clinically Integrated Home Monitoring (REF17)
  - This is a coordinated large-scale project in which telemedical home monitoring is being tested. The objective is to support a virtual and cross-sectoral collaboration between patients in their own homes, hospitals, municipalities and medical practices. The data collected from monitoring carried out by patients themselves is collected and shared in an cross-sectoral, inter-regional database.
- The Telecare North project (REF18)
  - This is a cross-sectoral collaboration between the 11 municipalities in northern Jutland, the North Denmark Region, general practitioners in Northern Denmark as well as Aalborg University to develop a telehomecare solution for patients suffering from chronic obstructive pulmonary disease (COPD) in northern Jutland. The solution is based on care and treatment in the patients' own homes with support from ICT. Part of the project involves collecting monitoring data on patients' lung function.
- The project to disseminate the use of telemedical ulcer assessment(REF19)
  - This dissemination project is a continuation of the demonstration project completed in 2010/2011 by Region Zealand and the Region of Southern Denmark. The project tested a telemedical solution comprising mobile phones with cameras and an electronic ulcer record for use in communication on the treatment of ulcers. The objective of the national dissemination of

telemedical ulcer assessment is to take the solution out to all the municipalities and regions as well as all relevant patients.

5.1.2 International experience

Denmark will be the first country in the world to implement the Continua Framework at national level. Other utilisation of the Continua Framework has been in local scenarios or in limited initiatives.

The report from the EU entitled ”ICT & Ageing – European Study on Users, Markets and Technologies 2010” (REF20) shows that, in around 2010, projects and initiatives in Europe and the US were all pilot projects with a high degree of silo-orientation. This also applied for Denmark, see section 3.1. Focus has now shifted to a larger geographic or national perspective in which standardisation and regulation are applied as parameters to achieve controlled and coherent structure and roll-out of solutions for health data collection. One of the tools in this process is application of international standards with a national profile in selected areas. Countries such as Germany, Britain and Finland have implemented initiatives with these characteristics.

Enrolment with Continua is on the rise, and the majority of suppliers of monitoring devices and associated products and services are now members of Continua. There are other associations for telemedicine solutions, but Continua is deemed to have the largest membership with regard to supporting standards and certification. Finished solutions which comply with Continua are also available, e.g. the Finnish Medixine solution (REF21).

At local level, several countries are working to launch solutions based on all or part of Continua. The Finnish Medixine is currently being launched as a health solution in DigiEcoCity, and implementation in China started in 2011.

The British National Health Service is analysing the possibility to utilise Continua in patient home care, as Continua is deemed to be a good supplement to IHE, for example.

The European Commission has completed an analysis of the technical possibilities to establish ”The eHealth Interoperability Framework” (REF22). In ten selected use cases, Continua and IHE have been assessed in relation to technical compatibility in a larger European context. Initially the IHE profiles have been recommended, as in a number of areas Continua does not align with the ten use cases and requirements from these. Primarily organisational aspects, i.e. openness regarding profiling and voting rights, were identified in the report as points where Continua should be improved. For example, only paying members can vote on a proposed profiling. The points have been submitted to Continua and several are already being implemented at Continua. It is expected that the other points will lead to changes or adjustments at Continua. The report also identifies a number of points which should be corrected at IHE. Details are in (REF22).

5.1.3 System picture to-be architecture

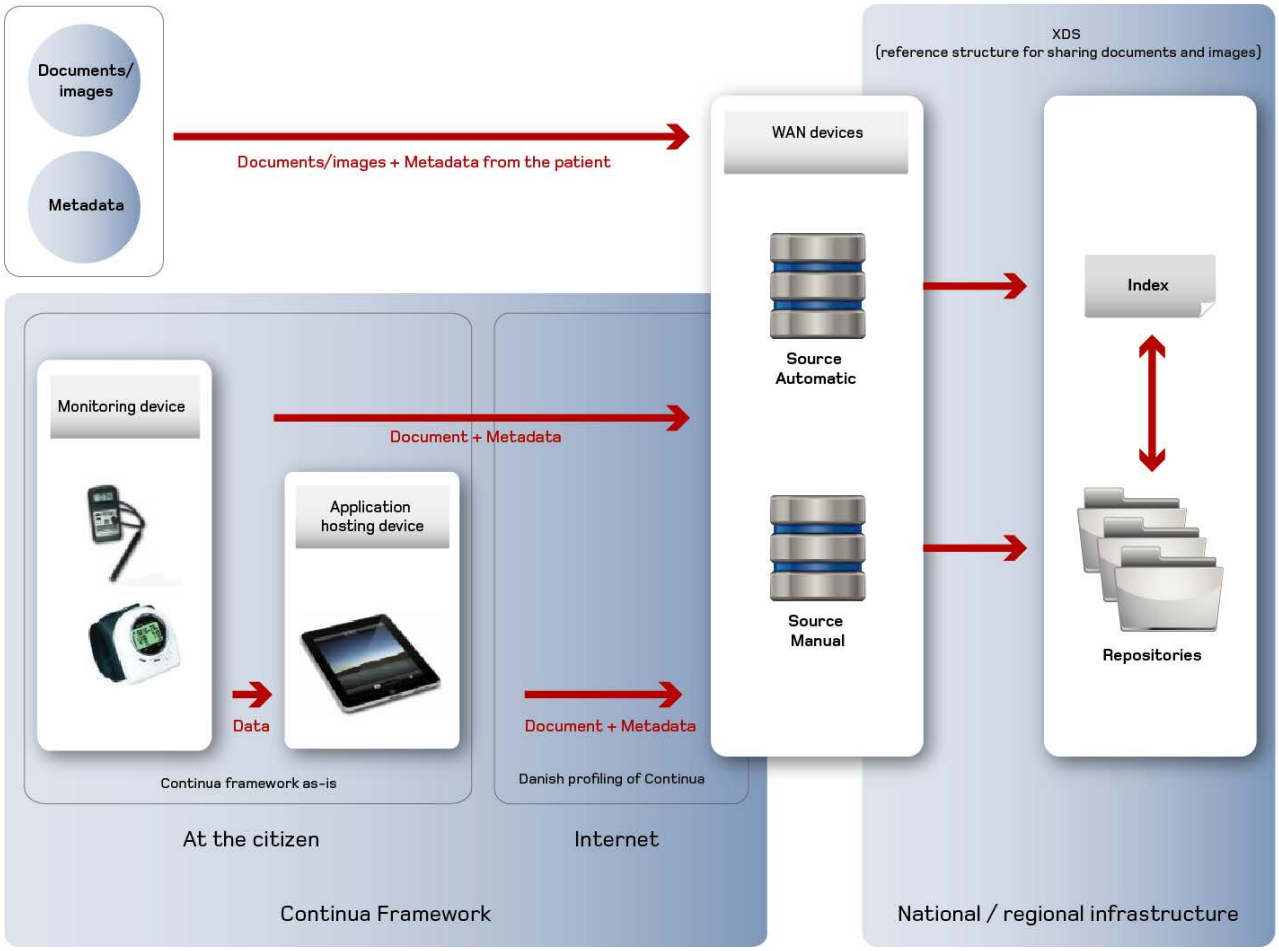


Figure 9Logical system-technical target image

In general terms, the figure describes the logical division in which the system-technical target image can be grouped and it gives a clear indication of the most important interfaces addressed by the reference architecture. The target image also aims at describing the system-technical framework for solutions to collect health data from citizens.

5.1.3.1 At the citizen's home etc.

With regard to the reference architecture, Continua's framework fully covers monitoring devices and delivery to the application hosting device, and the reference architecture adds no further specifications regarding location of functionalities or additions to interfaces.

Continua provides a certification scheme for monitoring devices and application hosting devices so that it is possible to document that the equipment meets the content and technical standards applied. The reference architecture has no certification requirements, but in connection with tendering procedures there is an option to place requirements on the suppliers that their equipment/devices must be Continua-certified.
When standards are set in relation to the reference architecture there will also be an option to include certification requirements, if relevant.

Collection of images as health data, e.g. for ulcer treatment and documents from citizens, is also outside of the Continua Framework, as illustrated in figure 9, and this collection has to be managed in parallel.

The application hosting device(s) are physically or virtually located with the citizen and carry out all data collection from monitoring devices so monitoring data is always sent to the WAN device by a application hosting device. The interface between monitoring devices and the application hosting device is specified and regulated solely by Continua. This exploits optimally work in Continua, in part through Continua profiling and in part through Continua's certification programme.

However, the reference architecture does make it possible to integrate the application hosting device and monitoring device in a combined unit, where the requirement is that the combined unit must be compatible with the interface to the WAN device.

The application hosting device manages transformation of specific formats from the monitoring devices under the Continua Framework to the general format specified for the interface with the WAN device and for setup of the metadata required.

5.1.3.2 WAN device

The WAN device is an important part of the system-technical goals, which establishes the coupling between collection of health data and consumption.

The WAN device has the following functional properties:

- Receipt of monitoring data from application hosting devices
- Enrichment of monitoring data and possible conversion to patient ID
- Ensuring that the required metadata is available and is correct for the monitoring data
- Acts as a document source for the XDS infrastructure
- Supplies metadata for searching in IHE XDS
- Implements coupling between secured and non-secured networks (the health data network which is used for communication between healthcare providers and the open internet)

There will be different WAN devices and the reference architecture places no requirements on the structure of these WAN devices. Therefore the structure has not been fixed and defined, but can be set in relation to the most suitable organisation of data collection.

A WAN device for an "organisation unit" is considered logical, as the number of physical units required is entirely up to the organisational unit, e.g. the municipality.

The interface for delivering monitoring data to the WAN device is described in more detail in the section below on communication, formats and metadata.

5.1.3.3 Other health data collection

Continua has been chosen as the framework for monitoring devices and application hosting devices, but the reference architecture also includes collection of monitoring data via other channels shown in the figure above as formulas to input information, questionnaires and images, but where collection is still by the citizen. The reference architecture does not describe how data is to be collected and processed locally, but dictates that the monitoring data collected must be delivered to a WAN device in a similar manner.

Health data collection via other channels could be through questionnaires completed by the citizen as preparation for treatment or a medical examination. For example this could be through the sundhed.dk portal, an app, or on the application hosting device at the citizen's home.

Images could be photographic records of ulcer treatment at home, from which nursing staff can monitor the treatment through images collected at the patient's home.

The same obligations apply for text and images, i.e. that they should to be able to make this data available in such a manner that it can be accessed using IHE XDS as described in the reference architecture for document and image sharing.

5.1.3.4 Formats for exchange of data

In the context of communication, there are various requirements relating to volumes of data and protocol overheads for the various interfaces illustrated in the system-technical target image. Monitoring data is enriched and consolidated in the transition from the individual interfaces, and this is again significant for the exchange format and content. Requirements vary from communication and band-width optimisation to more use-oriented optimisation.

5.1.3.4.1 Monitoring devices and application hosting devices

The data and exchange formats between the monitoring devices and the application hosting devices are specified in the Continua Framework by profiling the IEEE standards 11073-101, 11073-20601, and 11073-104xx. The reference architecture stipulates no further profiling with regard to using standards selected and profiled by Continua.

5.1.3.4.2 Formats for the WAN device

The reference architecture stipulates no single specific format which can be received by the WAN device, but it recommends that a representative set of standard formats be designated which covers the type of data collected. Selection should be made on the basis of international standards, possibly with elaboration through Danish profiling, if necessary. Using international standards means there is a wider range of possibilities regarding procurement and makes compliance with the required interface more likely.

Through work on the reference architecture and by studying the Continua Health Alliance framework, the following candidate exchange formats have been identified:

- PHMR, Personal Health Monitoring Report, is an HL7 CDA-2 based document specification which can contain the following types of health data:
    - Monitoring data from a monitoring unit
    - Notes or other types of free-text additions to monitoring data
    - Graphs and other data displays representing changes and trends in a citizen's health data

  Continua has taken part in work on preparing PHMR prototypes (REF23) and has developed a test tool for certification of compliance with the specification. Continua has prepared an implementation guide containing guidelines for IHE XDS based transport of the document and provides a certification process for data sources on compliance with the interface.

- An IHE PCD-01, Patient Care Device 01 transaction defines a very simple message mechanism whereby the application hosting device can transfer observations from monitoring devices. The objective is to keep processing by the monitoring device and application hosting device simple and thereby allow a health professional service to transfer the message to a CDA document. Use of PCD-01 requires data to be converted into a use-oriented document format, e.g. a Personal Healthcare Monitoring Report (PHMR) when delivering data to the XDS infrastructure.

5.1.3.4.3 Other channels to the WAN device

Questionnaires and other types of structured data can be stored in the required use format as soon as at data capture; structured as a document. The reference architecture points out that a CDA-2-based document specification is being prepared for questionnaire data and similarly collected data on the basis of IEEE 11073-10101 and IEEE 11073-10201.

5.1.3.4.4 WAN device (source) for XDS infrastructure

The format for this interface has been specified in the reference architecture for document and image sharing, as the WAN device has to manage provider properties and support the functionality for a document source. This means that data must be present in a document or image format.

5.1.4 Patient identification

The reference architecture stipulates a framework for patient identification to ensure that identification is completed and the collected health data is clearly linked to a patient before the health data is registered in XDS. Clinical consumption of collected health data requires this explicit identification. Anonymous health data or health data which cannot be coupled with a patient is outside the scope of this reference architecture.

As illustrated in Figure 9, health data is collected through different channels, monitoring devices, images and input/questionnaires. The specific characteristics of these channels are described in the table below.

Channel	Characteristics
Monitoring device	In most cases, monitoring devices will make an anonymous measurement of health data. Technological trends are in two directions such that some types of device are personal and thereby measurements from these are linked to the patient. Other units will always make anonymous measurements, and possibly without a unique device ID. This monitoring data requires reprocessing to link it to a patient. With the current technical possibilities it is not possible to have a fully secure personal ID, as biometric facilities, for example, have not yet been developed for large-scale use.
Images	Images from mobile phones etc. can be transferred using a personally identifiable ID or non-personally identifiable ID. If a non-personally identifiable ID is used, reprocessing of monitoring data will be necessary to link it to the right person ID (CPR no.).
Other health data collection (see section *5.1.3.3*)	Solutions within this spectrum should be designed so that patients identify themselves before starting to type in information, and the patientID is set before data capture commences, e.g. through NemID.

When patient identification takes place and when health data is coupled with a CPR number, depends on the balance between patient safety and information security, see section 7.6.

However, this requires that collected monitoring data is identified via a UUID (Unique User IDentifier) which is used to convert to a CPR no. For example, a UUID can be a device ID which gives a one-to-one relationship between monitoring data and patient, without the monitoring data being directly personally identifiable. The WAN device must have access to metadata which can be used to convert a UID to a CPR number.

If health data is collected via portal-based input, coupling to a CPR number should be at data capture, as there will be an active user-action in connection with the data capture.

Using monitoring devices, where patient identification is not carried out directly in connection with measurement will mean there is a need to classify monitoring data. This is dealt with in section 5.1.6.

5.1.5 Security

5.1.5.1 Roles and responsibilities

In the context of the reference architecture it is vital to clarify roles and responsibilities regarding hardware, software and data.

Initially, the system owner will be responsible for the hardware and software used in data collection. In some cases, the citizen could be required to purchase the equipment, but it will be the responsibility of the system owner to ensure that the equipment purchased complies with relevant requirements (including standards requirements).

If several users use the same hardware for their software, situations may arise where one system owner is responsible for its own software and for the hardware being used, while another is only responsible for its own software. In these situations it is important that there is clear agreement about who is responsible for what. This will also ensure that the citizen can have the necessary user support.

Data responsibility will always be with the person or authority acting as data controller. In many cases the system owner and the data controller will be the same (or belong to the same organisation), but there will certainly be many situations in which a system owner operates a system on behalf of a number of data controllers (e.g. a region which operates a system to collect data for citizens in all regions). In these cases it will be necessary to establish a data processing agreement between the data controllers and the system owner operating the system.

Data can be located in a data storage facility which is physically located outside the organisation of the data controller, but in this situation the data controller will remain the same and it will be necessary to establish a data processing agreement with the organisation operating the common data storage facility.

The citizen is instructed on use of the monitoring device etc. by the health professional or the responsible organisation, and in this context acts as a 'helper' for the health professional. The citizen should be informed about what data is to be used and who is to have access to the data in connection with the treatment. Furthermore, the citizen should be informed if data is to be forwarded on for other purposes than treatment. The citizen should have an opportunity to refuse to take part.

If a citizen has several application hosting devices or monitoring devices which 'belong' to different data controllers (e.g. the general practitioner and the homecare nurse), it should be very clear who is responsible for the individual (groups of) data collected.

Access of other health professionals to the data collected is regulated by section 42a of the Danish Health Act.

If the devices/equipment made available to the citizen belong to the data controller who initiated the data collection, there is a requirement that the application hosting device be subject to a security instruction which stipulates how the required level of security is to be been implemented. Annex C includes an assessment of the roles and responsibilities the working group has established for placing responsibility and the subsequent assessment of the important information-security risks.

5.1.5.2 Security of information

With regard to the fundamental elements in information security (accessibility, integrity, confidentiality, authenticity and non-repudiation), for health data collection at the citizen's home etc. integrity and confidentiality are the primary elements to be addressed.

In order to ensure confidentiality regarding personal data, the reference architecture recommends that data be made personally identifiable as late as possible and preferably not until the data is inside the national infrastructure, with its good security measures.

For reasons of patient safety, in some cases it is necessary to add a personally identifiable ID at an earlier stage and thereby ensure higher integrity of the data collected.

Therefore it is important that individual projects conduct a risk assessment covering the need to have clear identification of the person to whom the data relates while the data is still outside the national infrastructure. If personal identification is required outside the national infrastructure, the necessary security measures should be established to prevent unauthorised persons from having access to confidential information (see also REF5).

Another aspect relating to integrity is the issue of the correctness of data. In some cases, incorrect data could have consequences for patients' health or treatment and therefore it is important for projects to decide what consequences may arise from systematic display of incorrect data. If this poses a risk for the patient, security measures should be established to counteract risks of systematic display of incorrect data.

5.1.6 The validity of monitoring data

As described under patient identification, use of monitoring devices and application hosting devices raises a number of issues which the reference architecture must address. These issues all end in the credibility / validity of monitoring data for clinical consumption.

The reference architecture proposes a classification which states a level for how certain one can be that the measurement was actually taken on the person stated (UID etc.). An example could be a measurement that was supervised by a health professional from homecare services or similar. Another example could be that the device is personal and therefore it can be assumed that no others are using the device. The aim of the classification is to qualify the relationship between the patient and the measurement. Responsibility for preparation of this classification is national, while the system owner of the individual solution is responsible for ensuring application of the classification.

The credibility/validity of monitoring data should be determined on the basis of information/classifications aimed at a third party who verifies monitoring data during the measurement itself, as well as information/classifications aimed at the person to whom the measurement applies.

Verification authorisation - classification to identify a third party who verifies/guarantees the quality of the measurement (meaning in this context the truthfulness of the information regarding: time, place, person to whom the measurement applies, device and result). For example, this could be 'physician', 'nurse', 'other health professional', 'family member', 'none'.

Type of verification - classification which describes how the verification was conducted - could for example contain values such as 'physically present', 'remote monitoring and guidance', 'none'.

Identification of third party - unique identification of the person who verifies the correctness of the monitoring data.

Authority for identification of third party - identification of the body which made the identification of the third party. Could for example be 'public sector authorisation register', 'employee certificate', and 'none'.

Method for identification of third party - classification which indicates how a third party has identified himself in connection with the measurement. The classification could contain values such as 'biometry - fingerprint', 'biometry - eye scan', 'personal/employee certificate', 'technical signature', 'none' (default).

Personal verification - classification which describes the possibility for others to use the equipment/device than the person for whom the measurement applies. For example, could contain values such as 'not possible - sensors in pill/liquid form', 'not possible - device/sensors fitted to the body', 'possible - use of device requires biometric ID', 'possible - use of device requires ID', 'possible - use of device requires no ID'.

Personal identification - unique identification of the person on/for whom the measurement was made.

Authority for identification of person - identification of the body which made the identification of the third party. Could be 'Danish Civil Registration System', 'personal certificate', and 'none'.

Method for identification of person - classification which indicates how a person has identified him/herself in connection with the measurement. The classification could contain values such as 'biometry - fingerprint', 'biometry - eye scan', 'personal/employee certificate', 'technical signature', 'none' (default).

5.2 Technical implementation

5.2.1 WAN devices

The WAN device illustrated in the figure below is composed of several parts.

- A set of interfaces to which the collected health data can be delivered.
- A part which deals with setup of document formats with associated metadata and ensures unique patient identification and coupling to CPR number. This part is initially expected to be located in a non-secured network (possibly DMZ - Demilitarized Zone).

  A part which deals with functionality as a source in relation to the XDS infrastructure. This part receives documents and associated metadata and ensures correct implementation of XDS interfaces.

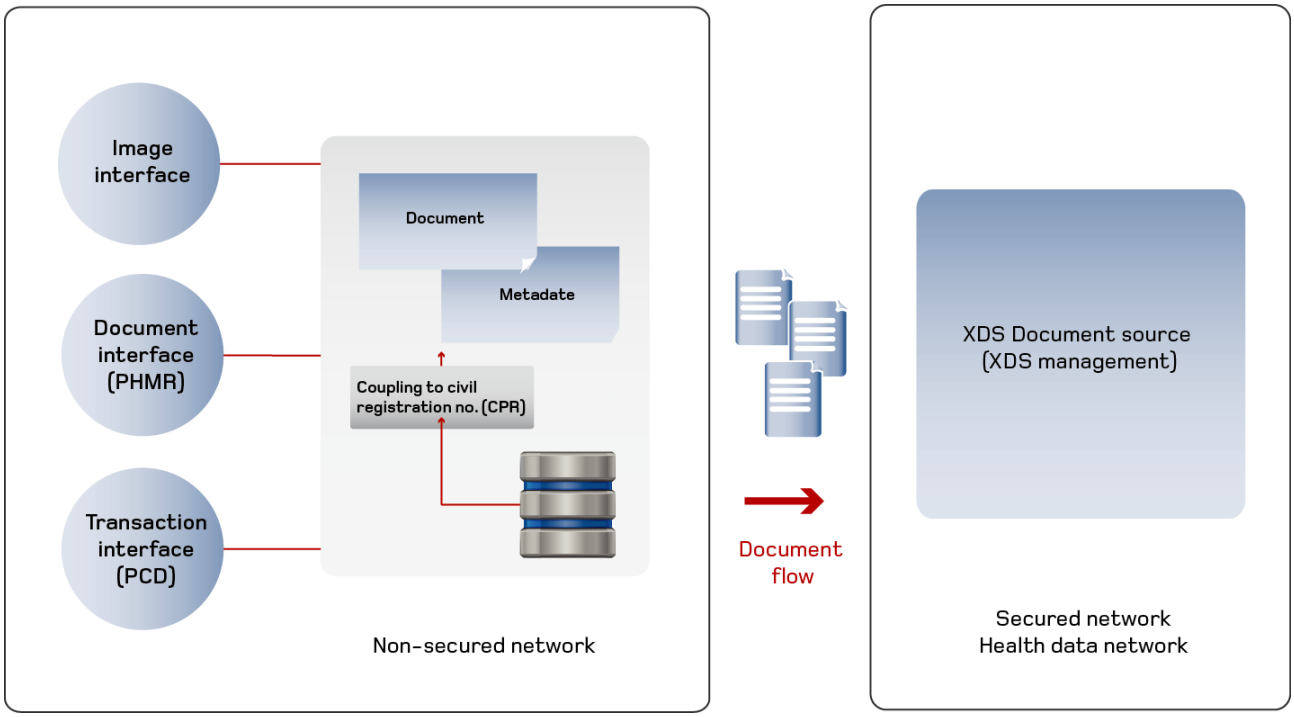


Figure 10 **WAN device**

See Continua guidelines (REF24) for specification of application hosting devices.

5.2.2 Interfaces

Communication between monitoring devices and the application hosting device complies with Continua and Continua's profiling of standards. The basis is IEEE 11073-20601 with associated device specialisations within IEEE 11073-114xx.

With respect to communication, Continua works with the concepts LAN/PAN which cover the following:

- LAN (Local Area Network) – Based on ZigBee, which is implementation of a wireless network with narrow band width and low energy consumption. Complies with IEEE 802.15.4 specifications.
- PAN (Personal Area Network) – Can be based on USB, i.e. cable link or wireless link via Bluetooth and NFC technologies.

Communication between the WAN device and the XDS infrastructure complies with the reference architecture for document and image sharing. If the data storage facility (repository) is not located on the health data network, communication should meet security requirements equivalent to those on the healthcare data network.

5.2.2.1 Interfaces to the WAN device

The WAN device must offer several options which as far as possible also support the associated metadata.

With regard to document-based health data, the reference architecture requires use of

- IHE XDR, Cross-Enterprise Document Reliable Interchange
- IHE XDM, Cross-Enterprise Document Media Interchange

as both IHE profiles support exchange of data and associated metadata.

PCD-based data (part of the Continua WAN interface). I.e. by using PCD-01 we are trying to comply with recommendations and profiling from Continua.

- IHE IT Infrastructure TF Vol 2 Appendix V Rev 6.0
    - WS-I Basic Profile over SOAP 1.2
    - WS-I Basic Security Profile, TLS and IHE ATNA

5.2.3 Standards and profiles

This section lists the standards recommended by the reference architecture

Standard/profile	Description	Profiling (if relevant) Relevant proposed profiling, e.g. measurement UUID, description of data validity, CPR no.
ISO/IEEE 11073-10101 Base Terms (Nomenclature)	Describes the nomenclature for the IEEE 11073 standard family	No profiling

ISO/IEEE 11073-10201 Domain information model	Standard which specifies the definition and structure for information exchanged between two parties within IEEE 11073- 20601.	No profiling
Standards covered by the Continua Framework	The Continua Framework covers a number of standards for both monitoring devices and interfaces to application hosting devices, WAN devices and patient systems. The list of standards is regularly updated and expanded.	No profiling
IHE PCD TF Vol1, Patient Care Device Technical Framework Volume 1	The IHE profile which describes the use of standards for integration regarding patient care devices. Volume 1 has an overall functional description and shows transaction flows.	No profiling
IHE PCD TF Vol2, Patient Care Device Technical Framework Volume 2	The IHE profile which describes the use of standards for integration regarding patient care devices. Volume 2 has technical descriptions of each transaction.	National profiling of PCD is conducted, i.e. clarification of the content of the format.
IHE PCD TF Vol3, Patient Care Device Technical Framework Volume 3	The IHE profile which describes the use of standards for integration regarding patient care devices. Volume 3 is a detailed specification of the contents and semantics.	National profiling of PCD is conducted, i.e. clarification of the content of the format.
HL7 Implementation Guide for CDA Release 2.0 Personal Healthcare Monitoring Report (PHMR)	Description and scope of CDA header and body for CDA documents containing patient health data, e.g. generated by monitoring devices.	National profiling of PHMR is conducted, i.e. clarification of the content of the format.
DICOM, Digital Imaging and Communication in Medicine	Standard for managing, storing and exchanging information in medical images. Describes formats and exchange protocols.	No profiling
IHE XDR, Cross-enterprise Document Reliable Interchange	XDR supports exchange of document-based data through a reliable message system/infrastructure. Recycles transactions from XDS.	No profiling
IHE XDM, Cross-enterprise Document Media Interchange	XDM supports document exchange using a common file and folder structure across different standard media.	No profiling

5.2.4 Metadata

The reference architecture recommends that a Danish profiling of metadata for health data be completed specifying where in the architecture metadata arises and where a conversion/transformation takes place if relevant.

For each metadata element used, the profiling should consider compatibility and origin on the basis of:

- Monitoring device
- Application hosting device
- WAN device, preferably as in section 5.2.1.

Metadata profiling and specification can benefit from being based on the metadata definition of XDS.

Annex B reproduces a matrix which can be used as a basis for profiling metadata.

5.3 Checklist of important properties

If a solution is to comply with this reference architecture, it should be possible to answer in the affirmative to the questions in the checklist below:

Area	Checkpoint	Reference
System-technical target image	Can all the components of the solution be embedded in the system-technical target image? Note: It is possible that several components of the solution will have to be embedded in the same element in the target image (e.g. a WAN device can contain devices and systems located at a private supplier and at an organisation acting as data controller). Similarly the same device can cover several elements in the target image (e.g. a device and application hosting device can be integrated).	Figure 9 in section 5.1.3
Data storage	Are clinically relevant measurements/datasets made available for other parties in the healthcare sector by regularly transferring this data to common repositories coupled to the national infrastructure (i.e. which can be accessed via XCA gateways on the health data network)?	Principle - health data which is to be used across specialists etc. Principle - use of national infrastructure.
Standards	Does the solution comply with/use the standards indicated in the reference architecture?	Section 5.2.3
Standards	Has a CDA-2-based document specification been prepared for questionnaire data and	Section 5.1.3.3 and section

	similar on the basis of IEEE 11073-10101 and IEEE 11073-10201, applicable for other data sources/channels than the monitoring devices and application hosting devices?	5.1.3.4.3
Certification	If there are requirements for Continua certification in connection with setting national standards or for procurement of monitoring devices and application hosting devices, are only Continua-certified monitoring devices and application hosting devices used?	Section 5.1.3.1 and section 5.1.3.4
Identification and security	If personal identification is necessary in the device or application hosting device, have the necessary security measures been established to prevent unauthorised persons from having access to confidential information?	Section 5.1.4 and section 5.1.5.2
Security	Has an information security risk assessment of the solution been completed?	Principle - collection and management of health data..... Section 5.1.5.2
Security	Have security measures been established to reduce risks to a level acceptable for data controller?	Principle - collection and management of health data..... Section 5.1.5.2

5.3.1 Checklist for implementation of the solution

Area	**Checkpoint**	**Reference**
Organisation	Have roles and responsibilities been clearly assigned?	Principle - clear division of responsibilities Annex C (Analysis of stakeholders) 5.1.5.1 (re. security - roles and responsibilities)
Data processing agreements	If another organisation than the organisation acting as data controller is responsible for operation of devices, WAN devices or common repositories, have data processing agreements been established that this organisation is to do the work on behalf of the data controller?	Principle - clear division of responsibilities Principle - collection and management of health data.....

Bibliography

REF01. *National Action Plan for Dissemination of Telemedicine*. June 2012. Fonden for velfærdsteknologi. http://www.digst.dk/Home/Velf%C3%A6rdsteknologi/Telemedicin%20og%20sundheds%20it/~/media/Files/Velfærdsteknologi/Telemedicinsk%20handlingsplan-web.ashx.

REF02. »Referencearkitektur - best practice anbefalinger.« 2013. *OIO Arkitekturguiden.* http://ea.oio.dk/referencearkitektur/best-practice-anbefalinger.

REF03. »Referencearkitektur.«*OIO Arkitekturguiden.* http://ea.oio.dk/referencearkitektur.

REF04. *Council Directive 93/42/EEC of 14 June 1993 concerning medical devices.* 14 June 1993. http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1993/L/01993L0042-20031120-en.pdf.

REF05. Reference architecture for sharing documents and images. http://www.ssi.dk/Sundhedsdataogit/National%20Sundheds-it/Standardisering/Referencearkitektur.aspx

REF06. Reference architecture for information security. https://bdkv2.borger.dk/Lovgivning/Hoeringsportalen/Sider/Fakta.aspx?hpid=2146003942.

REF07. »Continua: The Reference Architecture of a Personal Telehealth Ecosystem.« *Conference Publication, 12th IEEE International Conference on e-Health Networking Applications and Services (Healthcom) 2010.*

REF08. »Den fælleskommunale Rammearkitektur - KOMBIT, Kommunernes it-fællesskab.« *Local Government Denmark.* http://www.kl.dk/ImageVault/Images/id_55740/scope_0/ImageVaultHandler.aspx.

REF09. »New handheld mobile device performs laboratory-quality HIV testing.« *Healthcare IT News.* http://www.healthcareitnews.com/news/new-handheld-mobile-device-performs-laboratory-quality-hiv-testing?topic=08,16.

REF10. *National strategi for digitalisering af sundhedsvæsenet 2008-2012, Sammenhængende digital sundhed i Danmark.* December 2007. http://www.ssi.dk/Sundhedsdataogit/National%20Sundheds-it/~/media/Indhold/DK%20-%20dansk/Sundhedsdata%20og%20it/National%20Sundheds-it/Om%20NSI/SDSD_Strategi_2008_12.ashx.

REF11. *RSI: Telemedicinstrategi 2011*. 2011. http://www.regioner.dk/Aktuelt/Nyheder/2011/Juni/~/media/Filer/IT%20og%20Kvalitet/Sundheds-it%20diverse/Regionernes%20telemedicinstrategi_%202011_ny.ashx.

REF12. *Arkitekturprincipper for sundhedsområdet, Sammenhængende Digital Sundhed i Danmark, 2009*. u.d.

REF13. »Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.« 27. 06 2000. *Retsinformation.dk.* <https://www.retsinformation.dk/Forms/R0710.aspx?id=842.

REF14. »CONTINUA USE CASE LIFECYCLE PROCESS.« 2012.

REF15. »Telesår udbredelsesprojekt.« 2013 (project to disseminate the use of telemedical ulcer assessment). *MedCom.* http://www.medcom.dk/wm112455.

REF16. *For more detailed description (in Danish) see* http://www.continuaalliance.org/.

REF17. *Clinically Integrated Home Monitoring (KIH).* http://www.medcom.dk/wm112246.

REF18. *TeleCare North*. http://www.rn.dk/SundhedOgSygehuse/TeleCareNord/.

REF19. *Telesår udbredelsesprojekt (*project to disseminate the use of telemedical ulcer assessment). http://www.medcom.dk/wm112455.

REF20. *ICT & Ageing – European Study on Users, Markets and Technologies*. http://www.ict-ageing.eu/.

REF21. *Medixine Ltd. specializes in multichannel communication e-services for health care and wellness.* http://www.medixine.fi/.

REF22. *European Commission – ISA Work Programme. eHealth European Interoperability Framework (eHealth EIF).* Vers. Version 1.2. 18. 02 2013.

REF23. *Section 5: Implementation Guides*. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=33.

REF24. *The Continua Version 2012 Design Guidelines*. http://www.continuaalliance.org/products/design-guidelines.

REF25. *COUNCIL DIRECTIVE 93/42/EEC of 14 June 1993 concerning medical devices*. 14. June 1993. http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1993/L/01993L0042-20031120-en.pdf.

REF26. *Bekendtgørelse nr. 1263 af 15/12/2008 i henhold til Lov nr. 1046 af 17/12/2002: Bekendtgørelse om medicinsk udstyr*. <https://www.retsinformation.dk/Forms/R0710.aspx?id=122694.

REF27. »IT Infrastructure Technical Framework, baseret på Technical Framework - Revision 9.0.« 2012. *IHE.net.* http://www.ihe.net/Technical_Framework/index.cfm#IT.

Annex A Directive concerning medical devices

This reference architecture does not specifically relate to the quality of the medical devices used.

The requirements for medical devices are stipulated in **Council Directive 93/42/EEC of 14 June 1993 concerning medical devices** (REF25) with later amendments and additions. The Directive is currently being revised in order to strengthen regulation of medical devices. The Directive has been implemented in Danish legislation as Executive Order no. 1263 of 15 December 2008 (REF26).

The object of the Directive is to ensure:

"Harmonisation of national provisions concerning safety, health protection and performance characteristics of medical devices with a view to enhancing the free movement of goods, persons, services and capital".

Medical device means any instrument, apparatus, appliance, software, material or other article to be used specifically for diagnosis, prevention, monitoring, treatment or alleviation of disease[5].

Medical devices must satisfy the general requirements for construction and manufacture stipulated in Annex 1 of the Executive Order.

Medical devices are divided into four categories according to the risk they entail for the user[6]:

- Class 1 (low risk)
  - Includes non-invasive devices, invasive devices which are not surgical devices and which are intended for transient use, as well as certain types of therapeutic device.
- Class 2a (medium risk)
  - Includes certain types of surgically invasive device for short-term use, implants in teeth and active devices intended to supply or exchange energy or for use in diagnosis.
- Class 2b (medium risk)
  - For example surgically invasive devices for surgery or other active devices which are used short-term to supply ionizing radiation, have a biological effect, or are intended to administer medicines. In addition, certain types of implants and surgically invasive devices for long-term use.
- Class 3 (high risk)
  - Includes surgically invasive devices and implants used in the heart or central nervous system as well as devices which cause a chemical change in the body.

Devices in classes 2a and 2b require that the manufacturer's quality system is approved by a designated certification body. Devices in class 3 and certain types of device in classes 2a and 2b require the authorities to certify the product.

All types of device require the manufacturer to draw up a Declaration of Conformity stating that the device meets the requirements of the Directive and a technical specification of the device must be prepared.

[5] Section 1(2) of the Executive Order and Annex 1 (REF26).

[6] Annex 9 of the Executive Order (REF26).

The device must be furnished with a CE marking stating that it meets the requirements of the Executive Order. If a certification body has been involved in the approval process, it must be identified on the CE marking.

The revision of the Directive includes requirements to establish a common database to facilitate tracing of a medical device in the event that it does not satisfy the quality requirements. Similarly, the position of the certification body in relation to the manufacturer will be strengthened.

Annex B Input for metadata profiling

This annex contains a table which can act as starting point for profiling the metadata which can and must be included in HL7 PHMR and IHE PCD-01. All required metadata must be available in the XDS repository. Therefore it must be possible to state some metadata at the latest in a WAN device which itself may be a repository or it may deliver data to a repository.

An individual home-monitoring project can benefit from stating where in the process flow the metadata arises. The table also includes three columns headed: 'Monitoring device', 'application hosting device' and 'WAN device'. These are for the home monitoring project to document where metadata is set up in the process flow. The comments column is for an indication of the field's content.

The table is based on IHE XDS metadata, where the XDS role is 'Source' and metadata requirements are specified by an XDS index. Note that XDS works with two-sided requirements for metadata; a source side (XDS source) and a query side (XDS query). This reference architecture acts as the XDS source. More details on the metadata fields are in (REF27).

The codes used in the XDS column indicate:

- *R - Required; R2 - Required if Known*
- *O - Optional*
- *P - Registry is not required to support query of this attribute*
- *Cp - Computed/Assigned by Repository, required in register transaction*
- *Cg - Computed/Assigned by Registry.*

The 'WAN device requirement' states whether metadata is to be inserted in a Danish profile (*K – krævet (required)*). It is deemed that a Danish profiling should comply with all the IHE *R-requirements* and that there could be further needs to tighten up the standard's metadata in Danish profiles.

Metadata field	**XDS requirement: code** [7]	**Monitoring device**	**Application hosting device**	**WAN device requirement:**	**Comments**
classCode	R			K	Overall type of document [8]
classCodeDisplayName	R			K	Can be Danish names[8]
typeCode	R			K	Detailed type of document[8]
typeCodeDisplayName	R			K	Can be Danish names[8]
eventCodeList	O				
eventCodeDisplayNameList	O				
serviceStartTime	R2			K	
serviceStopTime	R2			K	
Title	O				
Comments	O				
confidentialityCode	R			K	
confidentialityCodeDisplayName	R			K	

[7] R - Required; R2 - Required if Known; O - Optional; P - Registry is not required to support query of this attribute; Cp - Computed/Assigned by Repository, required in register transaction; Cg - Computed/Assigned by Registry

[8] NSI's suggestions for use of classCode and typeCode, respectively, as a result of the NPI/HealthCare project.

Metadata field	XDS requirement: code [7]	Monitoring device	Application hosting device	WAN device requirement:	Comments
Author (section)[9]					
authorInstitution (sub-attribute for author)	R2			K	
authorPerson (sub-attribute for author)	R2			K	
authorRole	R2			K	
authorSpecialty	R2			K	
legalAuthenticator	O				
healthcareFacilityTypeCode	R			K	
healthcareFacilityTypeCodeDisplay Name	R			K	
practiceSettingCode	R			K	
practiceSettingCode DisplayName	R			K	
repositoryUniqueId	Cp				
URI	Cg			K	
patientId	R			K	Civil registration number (CPR no.)[10]
sourcePatientId	R			K	
patientName	R			K	
patientGender	R			K	
patientDateOfBirth	R2			K	
patientAddress	R2			K	
availabilityStatus	Cg				
creationTime	R			K	
entryUUID	Cg				
uniqueId	R			K	
formatCode	R			K	
formatCodeDisplayName	R			K	
Hash	Cg				
homeCommunityId	O				
languageCode	R			K	
mimeType	R			K	
Size	Cg			K	

Annex C Roles and responsibilities

Annex C is the result of a workshop held by the working group on roles and responsibilities in connection with health data collection from citizens.

[9] Notes on the author section: The author could be the organisation which ordered the home monitoring or the organisation which processes the data received in an application hosting device. The author is considered as stated when either authorPerson or authorInstitution has been stated. With regard to authorInstitution, SOR or SHAK should be used. For authorPerson, CPR no. should be used to identify the health professional where this is possible.

[10] Patients under home monitoring are always stated with their CPR no.

The Annex is a preliminary version and will be revised when a new system of concepts for information security and a system of concepts for telemedicine have been drawn up.

Task/role	System owner	Data controller	Health professionals involved in treatment pathway	Other health professionals	Citizen	Relations/helpers	Others
Hardware							
Set up of device	A				K		
Support and maintenance	A	K		I	I	I	
Guidance on use (preparation)	A		K [11]		I	I	
Error report (the person who finds the error is responsible for reporting it)							
Purchase or replacement of device	(A)12				(A)		
Establishment of agreements with 'supplier/executor'	A				I		
Software							
Helpdesk	A	K	I	I	I		
Support	A	K	I	I	I		
Specialist health instruction (incl. description of performance level)			A	(I) [13]			
Error report (the person who finds the error is responsible for reporting it)							
Installation	A						
Establishment of agreements with 'supplier/executor'	A						
Data							
Data input (for deviations - if data is not notified or there is an error)	U	A					
Processing of data received centrally		A					

[11] If they take part in the measurement

[12] But responsible for preparing the positive list of possible devices, if the citizen is to buy him/herself.

[13] If necessary for performance of their task.

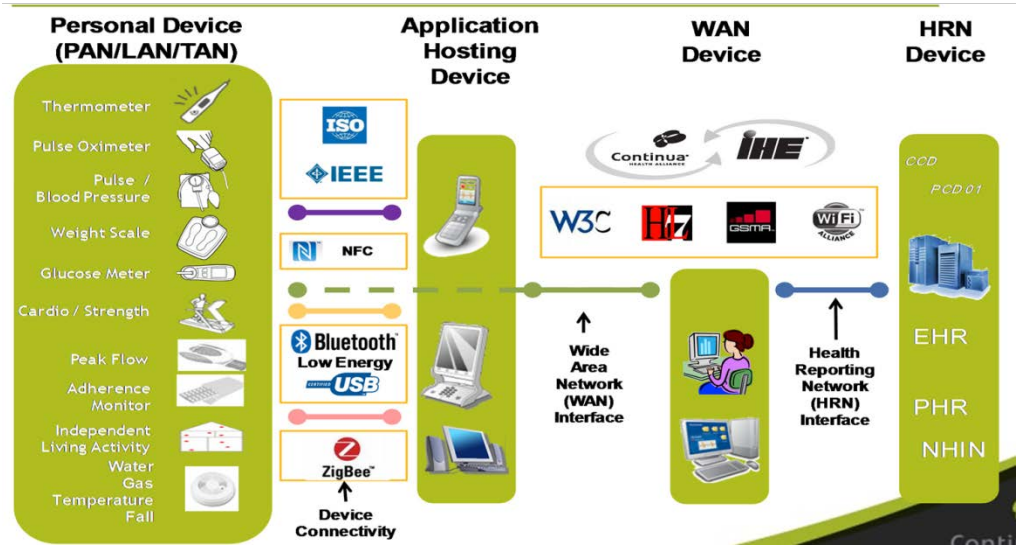
Task/role	System owner	Data controller	Health professionals involved in treatment pathway	Other health professionals	Citizen	Relations/helpers	Others
Establishment of agreements on data consumption	U	A					

A=Responsible (ansvarlig)
U=Executor (udførende)
K=Coordinated with (koordineret med)
I=Informed about

Annex D Continua Health Alliance

Continua Health Alliance is a non-profit association composed of about 200 companies and other organisations working with health technology. The aim is to create better opportunities to exchange data from monitoring devices between healthcare providers and between the healthcare sector and citizens.

The Continua Framework is illustrated in the figure below, and it describes the use, composition and profiling of a number of standards which together make up a consistent foundation for collecting and exchanging health data measured via various monitoring devices and application hosting devices, and which ensure interoperability between devices and components. The Continua Framework comprises monitoring devices and application hosting devices, WAN devices and onwards to the specialist eHealth solutions.



Continua develops standards for the products' mutual compatibility so that monitoring data can be transported from data-exchanging medical or welfare equipment/devices (blood-pressure monitors, blood-glucose meters, personal scales etc.), the associated ICT systems and onwards to the ICT solutions used by health professionals.

The standards are based on ISO/IEEE standards, but they focus exclusively on standardising data exchange via Bluetooth, WLAN and similar.

Continua issues design guidelines which refer to the standards and specifications on which Continua bases itself to ensure interoperability. Design guidelines have been drawn up for the interface between monitoring devices and the application hosting device and for the interface from the application hosting device to the WAN device.

Continua has established a product certification programme under which enterprises can have their products certified. The products are tested at one of Continua's test laboratories and after the test they can be placed on the market as *Continua Certified Products.* The objective of the product certification programme is to ensure interoperability between devices and application hosting devices.