ETSI TR 103 477 V1.3.1 (2023-01)

eHEALTH;
Standardization use cases for eHealth

Reference
RTR/eHEALTH-0009v131

Keywords
eHealth, HEALTH, interconnection, interoperability, interworking, privacy, security, usability, use case, user

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee eHealth (eHEALTH).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document presents a number of typical use cases in the eHealth domain and their analysis to identify gaps in standardization. The analysis covers aspects of link connectivity, network interconnectivity, semantic and syntactic interoperability, security (risks and provisions) and the existence of standards to meet each aspect. Furthermore the analysis identifies actors and their roles, for each of primary, secondary and tertiary involvement in the use case.

The use case examples have been drawn or informed by publications from industry, from completed FP7 and H2020 projects, from ETSI Technical Bodies, and from current eHealth and Health industry practices.

The update in V1.2.1 of the present document added therapeutic use cases in addition to the baseline diagnostic use cases of the previous edition (V1.1.1), and the update in the present version (V1.3.1) adds consideration of data for machine based processing and non-clinical medical use cases.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 118 501: "oneM2M Use Case collection".

[i.2] EC Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market.

[i.3] ETSI TR 102 764: "eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth".

[i.4] World Medical Association International Code of Medical Ethics.

NOTE: Available at https://www.wma.net/policies-post/wma-international-code-of-medical-ethics/.

[i.5] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0024.

[i.6] GDPR: "General Data Protection Regulation (GDPR) (EU) 2016/679".

[i.7] Void.

[i.8] Void.

[i.9] ISO/IEC 7498-1:1994: "Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model".

[i.10] IEC 60906-2: "IEC system of plugs and socket-outlets for household and similar purposes - Part 2: Plugs and socket-outlets 15 A 125 V a.c. and 20 A 125 V a.c.".

[i.11] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications (Text with EEA relevance).

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0036.

[i.12] World Health Organization International Health Regulations.

NOTE: Available at https://www.who.int/health-topics/international-health-regulations#tab=tab_1.

[i.13] Infectious Disease (Notification) Act 1889.

NOTE: Text of this act is available at https://www.legislation.gov.uk/ukpga/Vict/52-53/72/enacted.

[i.14] UK Government notifiable diseases website.

NOTE: Available at https://www.gov.uk/government/collections/notifications-of-infectious-diseases-noids.

[i.15] ETSI GR SAI 007: "Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

asset: anything that has value to the organization, its business operations and its continuity

care services: all services and goods provided with the aim of preventing, alleviating, curing or healing human illness and physical and/or cognitive impairments

causation: indication that one event is the result of the occurrence of the other event

NOTE: I.e. there is a causal relationship between the two events.

clinical staff: professional caregivers, responsible to deliver care services to patients, including care specialists and care institution managers

correlation: statistical measure (expressed as a number) that describes the size and direction of a relationship between two or more variables

exergaming: combination of exercise and game

NOTE: I.e. using games as a means of exercising.

General Practitioner (GP): medical doctor qualified to practice medicine, responsible for medical treatment

nurse: professional caregiver responsible to deliver care services to patients, including giving medical and other attention

physician: person qualified to practise medicine

NOTE: This particularly refers to a health professional who specializes in diagnosis and medical treatment as distinct from surgery.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Alternating Current
AF	Atrial Fibrillation
AI	Artificial Intelligence
ATM	Asynchronous Transfer Mode
BAN	Body Area Network
CE	European Community
CIA	Confidentiality, Integrity and Availability
CIM	Context Information Management
DC	Direct Current
EC	European Commission
ENISA	European Network and Information Security Agengy
EU	European Union
FP7	Framework 7 Projects
GDPR	General Data Protection Regulation
GoS	Grade of Service
GP	General Practitioner
HIV	Human Immunodeficiency Virus
HR	Heart Rate
HRM	Heart Rate Monitor
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISG	Industry Specification Group
ISM	Industrial Scientific Medical
ML	Machine Learning
MTBF	Mean Time Before Failure
MTTR	Meant Time To Repair
NIS	Network Information Security
OSI	Open Systems Interconnection
QoS	Quality of Service
RHR	Resting Heart Rate
SAI	Securing Artificial Intelligence (ETSI ISG)
SAREF	Smart Applications REFerence ontology
UK	United Kingdom (of England, Scotland, Wales and Northern Ireland)
UNCAP	Ubiquitous iNteroperable Care for Ageing People
WHO	World Health Organization
WMA	World Medical Association

4 Introduction to eHealth use cases

4.1 Structure of use cases

NOTE 0: In the present document names are given to the actors, often Alice, Bob (as affected actors) and Eve (often representing an adversary). The use of such names are not intended to convey gender roles but are only used as an alternative to using terms such as Party-A, Party-B and so on.

Use cases are developed to examine problem statements that are a concise description of issues that need to be solved in the context of the use case. The purpose of the use case is to clearly describe:

- What the problem is.
- Who has that problem i.e. who will benefit when it is solved.
- What are the consequences of the problem.

- What a possible solution would be, this sets the expectations and the scope of the solution (is it a new process, an application, etc.).

In the context of standardization the problem is multi-fold but is primarily concerned with determination of interoperability. This may be at the application level where syntactic and semantic coherence is critical, or at any of the layers of the OSI stack (see ISO/IEC 7498-1 [i.9]). For communications interoperability the main concerns are to give assurance of connectivity, of routing (i.e. the ability of devices to connect in order to provide reliable transport of information from source to sink), and of mutuality of transfer rates (i.e. to ensure that data produced at a given rate can be consumed at the same rate).

In any large and interdisciplinary problem space there are many stakeholders involved. For the purposes of use case modelling these stakeholders are identified as actors with one or many roles to play in each scenario that is represented. The use cases are structured in particular with the focus on interoperability in order to identify where standards are required to fulfil the use case. This is especially true when the solution aims to provide functionalities and processes in the medical context, which involve collection of medical and other personal data, and acting upon that data or even using it to provide treatment. Thus, it is of highest importance to identify as many stakeholders as possible that are in any way involved in the problem and who will be resultant stakeholders in the solution. This includes both primary stakeholders, who will be directly affected by the solution, as well as secondary stakeholders that will only feel the results indirectly. Stakeholders can be both individuals and organizations, and should in addition to the entities accepting care (the patients) and the entities providing care (care providers, nurses, physicians) also include the supporting entities and controlling entities. The latter two groups encompass the manufacturers, equipment vendors, solution providers, developers, distributors, payers; and regulators, agencies, committees, boards and unions.

For practical reasons the role of machines and the interconnection of machines in eHealth is particularly important.

The use cases in the present document complement the Machine-to-Machine use cases for eHealth found in ETSI TR 118 501 [i.1]. Further, the use cases in the present document extend the model presented in ETSI TR 102 764 [i.3] beyond the purely communications model in which for each use case consideration was given to identification of the originating and terminating parties for the eHealth **communication** as follows:

- Patient originated: Health Professional terminated (noting that the Health Professional could be equipment rather than a person).
- Health Professional originated: Patient terminated.
- Health Professional originated: Health Professional terminated.
- Patient to Health Professional dialogue.
- Health Authority to Citizen (Health Authority originated: Citizen terminated).

In addition the present document extends the view of eHealth intervention which may invoke each other:

- Telemedicine.
- Remote monitoring.
- Mobile monitoring.
- Therapy intervention.
- Emergency intervention.
- Wellness monitoring.

NOTE 1: Monitoring wellness activity is not considered a medical monitoring activity but may be used to supplement information presented to a health professional. Furthermore a wellness monitor is not expected to be classified as a medical device (see Annex B).

- Exergaming.

NOTE 2: Exergaming, the role of games in exercise, is not considered a medical intervention and as such the equipment involved and the results logged are not expected to be classified as medical devices (see Annex B) but the record of the activity may be made available to a health professional in support of a diagnosis or treatment session.

The present document refreshes the model used in classification of the communications requirements from [i.3] in expanding the use cases:

- Unidirectional (including broadcast).
- Acknowledged uni-directional (unicast and multicast).
- Symmetric bi-directional (unicast).
- Asymmetric bi-directional (unicast and multicast).

In eHealth it is anticipated that a significant proportion of the communication will be between actors where the actor is a machine, for example, between monitoring equipment, e.g. a BAN sensor, and eHealth middleware; the Health professional will receive alarms and will when necessary or convenient access the information (where the distinction between necessary or convenient will be determined in part by the priority of the message and by the pre-processing of the message content).

In instances where the health professional is represented by proxy, and where the proxy is an Artificial Intelligence (AI), or where AI is used in the processing of data to offer guidance to the health professional, the use case should clearly identify the role of AI.

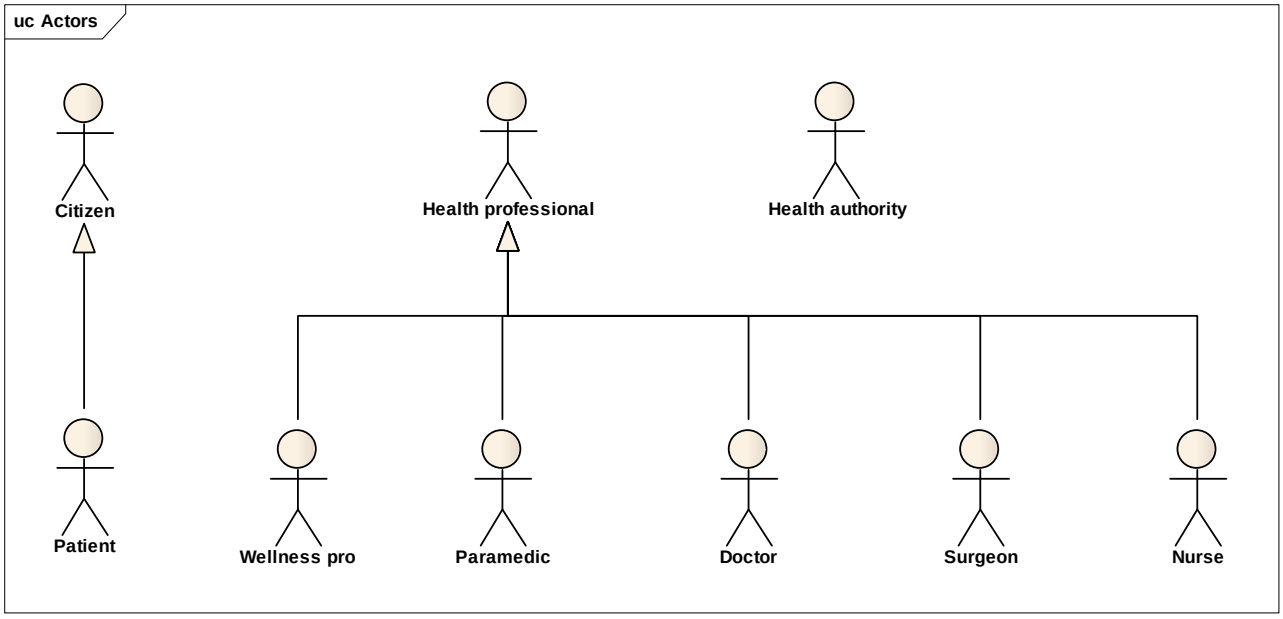
4.2 Actors and roles

In the eHealth context the obvious actors are those from the medical intervention group and thus Doctors, Nurses, Surgeons and the many specialisms are covered. However, eHealth is not simply about medical professionals and thus the stakeholders and the actors representing them should include standards bodies, operators, manufacturers, regulators and governments (national, regional and international) and of course medical sensors and intervention devices. In addition, as health and healthcare is a significant cost item there will be instances where medical insurance companies, administrators of medical facilities, research analysts and others will require access to health data.

The purpose of access to eHealth data and services is not simple to categorize. For example, in addition to diagnostic medicine and care, it is also necessary to identify effectiveness of treatments, of the how diseases spread and so forth. The consequence is that the set of actors in eHealth both by role and by name has to be mutable over the lifetime of the system.

The set of actors described in the present document extends the model presented in [i.3] in order to address changes in the eHealth landscape. In particular the consideration of specialist forms of eHealth professional and of patients as citizens is extended to consider the role of machines in the eHealth environment.

NOTE: The list of eHealth actors is indicative and is not considered as complete.



NOTE: Each actor may be represented by a machine (i.e. a doctor does not need to be a human being).

Figure 1: Actors in use cases for eHealth analysis

In addition to the patient being a simple case of a citizen suggested in Figure 1 the patient may also be represented by 3rd parties that may include carers and wellness agents. Where an actor is represented by a 3rd party the 3rd party may also be an instance of an AI enabled service. In such cases the authority of the 3rd party to act on behalf of the patient may be represented as shown in Figure 2.

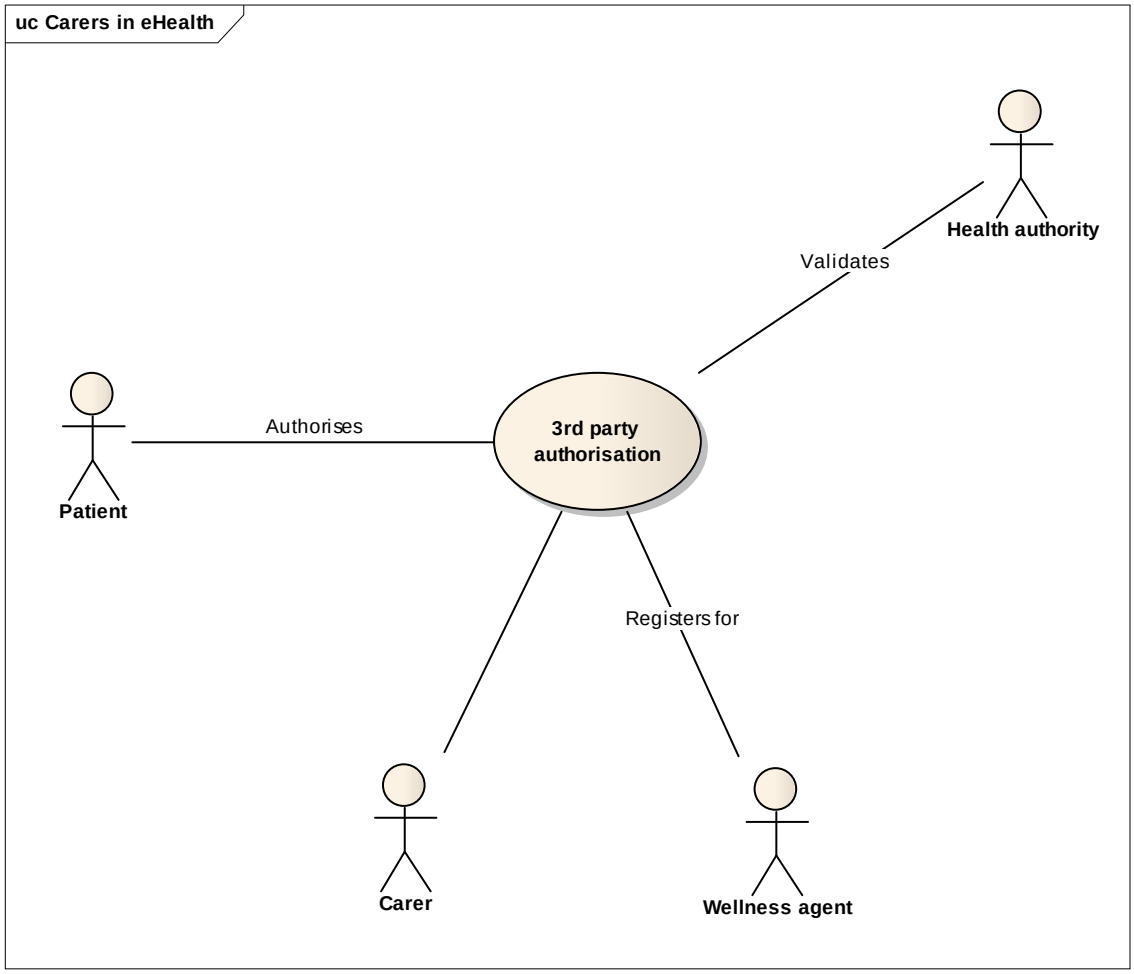


Figure 2: Example of carers and like actors being authorized by patient

Within the definition of health authority considerations have to be given to public health policy and the role of various forms of environmental control. With respect to the communications scenario "Health Authority to Citizen (Health Authority originated: Citizen terminated)" there may be broader policy constraints imposed as suggested in Figure 2a with respect to the role of health policy and its implementation through Governmental authorities.

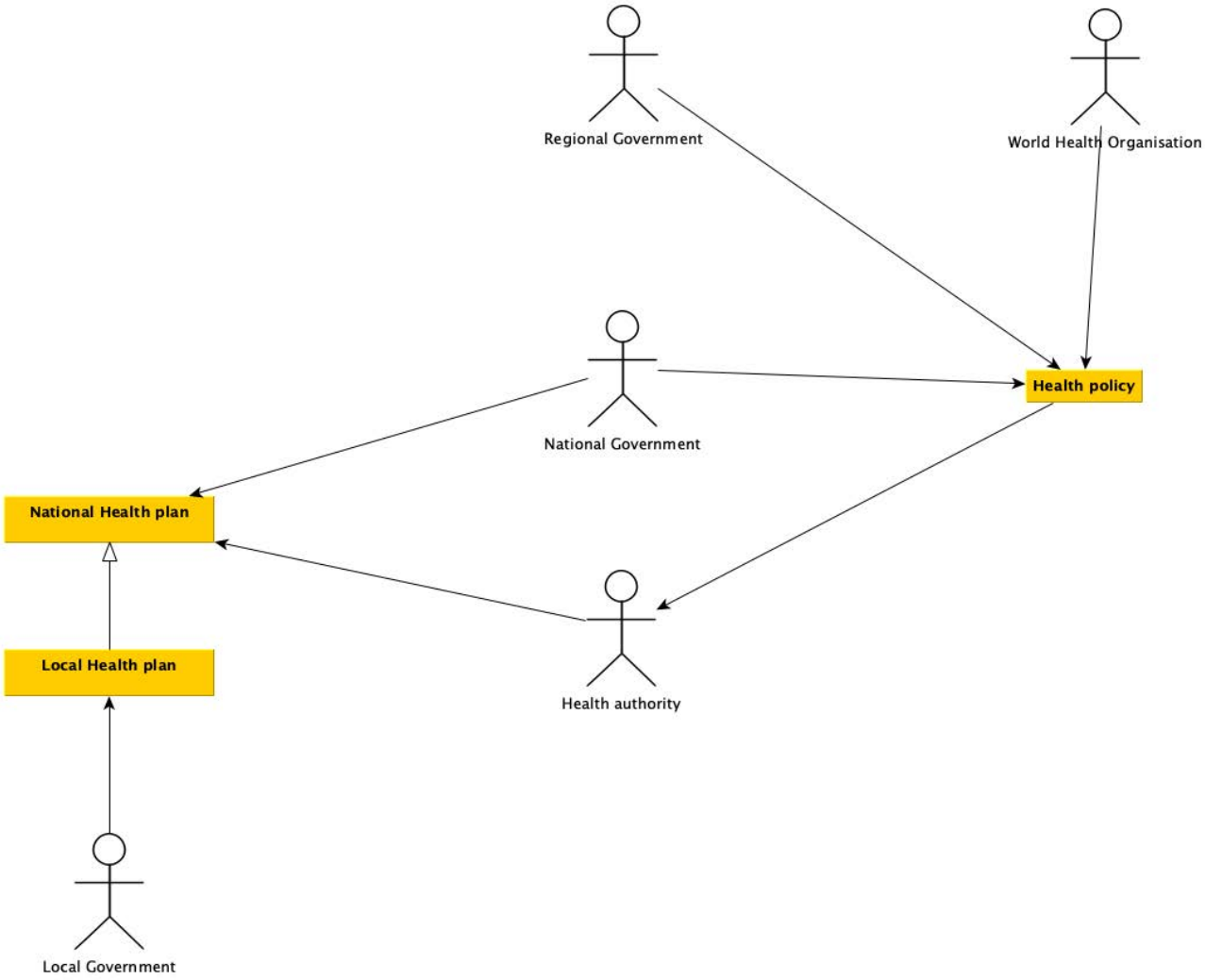


Figure 2a: Governmental level actors relationship to health policy and planning

One further group of actors that are instrumental in health but that are only indirectly addressed in the patient to health professional relationship are the pharmaceutical industry, and the health device industry. The roles of these actors is addressed in part in clause 6 and clause 7 with respect to the abstract use case for each of diagnosis and therapeutic or clinical intervention.

4.3 Time and performance constraints

eHealth is a global phenomenon and will require that data is passed across borders without undue delay. Any constraints on processing speed, network transfer rate and data lifetime should be identified in the use case analysis.

For the purposes of analysis a border is not limited to a national (geographic or political) border but may also refer to the interface between equipment and between services. For some geographic domains specific constraints and obligations apply including those for eHealth data in Europe Directive 2011/24/EU [i.5] applies. For data that is not specifically eHealth data in the scope of Directive 2011/24/EU [i.5] the wider provisions of the GDPR [i.6] and equivalent regulation would be expected to apply.

4.4 Forms of interoperability

4.4.1 Syntactic interoperability

Syntax derives from the Greek word meaning ordering and arrangement. The sentence structure of subject-verb-object is a simple example of syntax, and generally in formal language syntax is the set of rules that allows a well formed expression to be formed from a fundamental set of symbols. In computing science syntax refers to the normative structure of data. In order to achieve syntactic interoperability there has to be a shared understanding of the symbol set and of the ordering of symbols. In any language the dictionary of symbols is restricted, thus in general a verb should not be misconstrued as a noun for example (although there are particularly glaring examples of misuse that have become normal use, e.g. the use of "medal" as a verb wherein the conventional text "He won a medal" has now been abused as "He medalled"). In the context of eHealth standardization a formally defined message transfer syntax should be considered as the baseline for interoperability.

4.4.2 Semantic interoperability

Syntax cannot convey meaning and this is where semantics is introduced. Semantics derives meaning from syntactically correct statements. Semantic understanding itself is dependent on both pragmatics and context. Thus a statement such as "Patient-X has a heart-rate of 150 bpm" may be syntactically correct but has no practical role without understanding the context. Thus a heart-rate of 150 bpm for a 50-year old male riding a bike at 15 km/h up a 10 % hill is probably not a health concern, but the same value when the same 50-year old male is at rest (and has been at rest for 60 minutes) is very likely a serious health concern. There are a number of ways of exchanging semantic information although the success is dependent on structuring data to optimize the availability of semantic content and the transfer of contextual knowledge (although the transfer of pragmatics is less clear).

There are a number of existing ontologies in eHealth but there does not appear to be a (single) global standard for the transfer of semantic data within a common syntax. There is therefore a challenge to resolve the means to transfer semantic knowledge with representation of both context and pragmatics.

ASSERTION: Semantic interoperability is essential to allow machine based eHealth intervention.

NOTE: The ETSI SmartM2M group is supporting standardization of the SAREF ontology and this may be considered as a starting point for an eHealth ontology (http://ontology.tno.nl/saref/).

4.4.3 Electrical and mechanical interoperability

Quite simply a device with a power connector using, for example, a Type- IEC 60906-2 [i.10] connection cannot accept power from anything other than a IEC 60906-2 [i.10]. Similarly, for example, a serial port complying to USB-Type-A will not be able to connect with a USB-Type-C lead. In addition to simple mechanical compatibility there is a requirement to ensure electrical interoperability covering amongst others the voltage level, amperage level, DC or AC, frequency if AC, variation levels and so forth.

4.4.4 Radio communication interoperability

In the eHealth environment devices have to be able to interconnect and if wireless communication is deployed then it is obvious that the communicating end-points use the same means to communicate. In the radio sense this means sharing knowledge of frequency band, modulation technique, symbol rate, power, and so forth. The current Industrial Scientific Medical (ISM) band allocations are in this respect not strongly protected and many non-ISM devices use the ISM bands ("A" bands are allocated to ISM applications, "B" bands may be used by ISM and non-ISM applications).
A consequence of the current management of the ISM bands is that knowledge of the frequency does not determine modulation waveform and vice versa.

4.4.5 Mutual understanding of vocabulary

Any term in eHealth has to be clearly and unambiguously understood. The requirements for syntactic and semantic interoperability described above apply. In addition the glossary of terms introduced in Annex D (Extended glossary of terms) of the present document also apply.

5 eHealth objectives and high level requirements

5.1 ICT centric requirements

In ETSI TR 102 764 [i.3] a statement was made of the objectives that an eHealth system should be designed to meet. Whilst the statements in ETSI TR 102 764 [i.3] were primarily derived from analysis of the network requirements for eHealth the present document also addresses the data and user management aspects of an eHealth system. The objectives stated in ETSI TR 102 764 [i.3] are reflected in the present document and updated in Table 1 to address changes in the technology and regulatory environment and to address the wider scope of the present document.

Table 1: Mapping of eHealth objectives and requirement class

Objective to meet	Resulting requirement class
A user should expect ubiquitous network connectivity.	Reliability and availability (network interoperability)
The user should reasonably know that eHealth equipment that requires to be connected through a network should be able to access the network.	Availability
The eHealth system should support the interworking of heterogeneous devices and networks.	Network interoperability
An eHealth device should be able to interact securely with the eHealth infrastructure.	Security: Availability
Information held within an eHealth device should be protected from unauthorized access, modification and destruction.	Security: Availability; Security: Integrity
Services provided within the eHealth infrastructure should be available only to authorized users of the eHealth system.	Security: Availability (authorization)
Information sent to or from a registered user of the eHealth system should be protected against unauthorized or malicious modification or manipulation during transmission.	Security: Integrity
Information sent to or from a registered user of the eHealth system should not be revealed to any unauthorized 3rd party.	Security: Confidentiality, Security: Availability (Access control); Security: Confidentiality
An eHealth user should be able to communicate confidentially with other users within the eHealth network.	Security: Confidentiality, Privacy
Details relating to the identity of an eHealth user should not be revealed to any unauthorized 3rd party within the eHealth network or in the wider ICT networks.	Security: Availability (Access Control), Security: Availability (Identity Management), Security: Confidentiality, Privacy
Access to the operation of services by authorized eHealth users should not be prevented by malicious activity within the eHealth network or in the wider ICT networks.	Availability
The eHealth system should be able to collect information relating to the context of any eHealth transaction.	See ISG CIM work
The eHealth system and the devices used to access it should allow any member of society to be able to use the system.	Availability, User system interaction

5.2 Person centric health eco-system

The objectives and requirements related to the eHealth system identified in clause 5.1 above are unfortunately incomplete and in part this is a consequence of lack of semantic and syntactic interoperability, and to an extent poor understanding of contexts of health measurement. A simplified concept relationship diagram is shown in Figure 3.

However, there are a large number of questions that have still to be posed and answered: Does trauma (say a broken bone) mean the person suffering the trauma is unhealthy? If a health professional is involved in treatment of trauma it will be recorded in the documentary health record. Multiple instances of repeated trauma may imply other health issues, however there may be only indirect causal links. Thus, whilst smoking may lead to a higher propensity to respiratory disease there is no evidence proven link that a smoker will end up with a respiratory disease.

The assertions in Figure 3 are quite strong: Behaviour modifies health and health modifies behaviour. Or in alternative terms running naked in the snow may lead a person to catch a cold, and having a cold may make it less likely for that same person go out and run naked in the snow. However there is a strong requirement in medical diagnosis to not confuse correlation and causation. This is particularly important for statistical based machine processing where chosen data sources may identify strong correlations but miss causation if appropriate data sources are not selected.

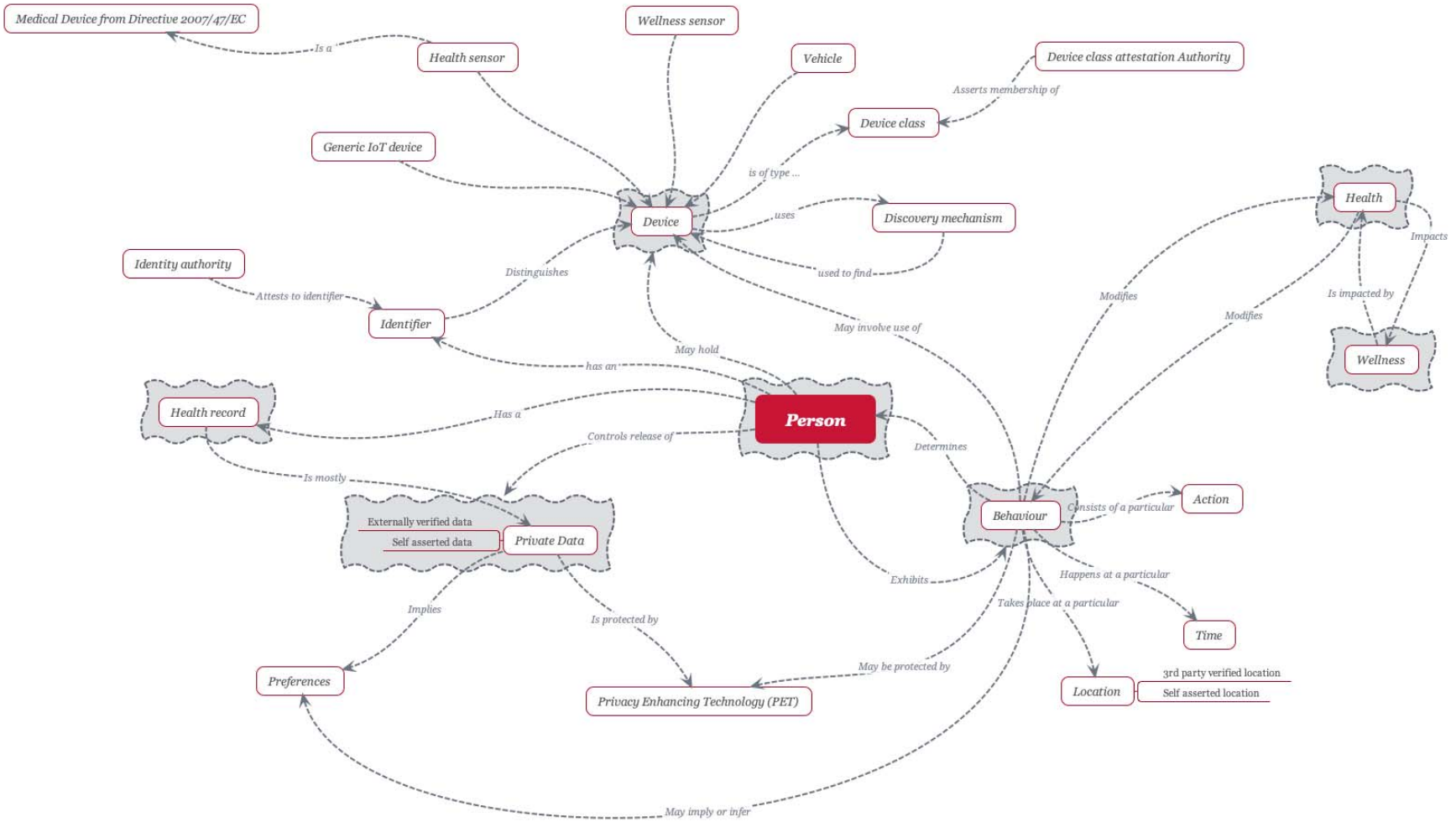


Figure 3: Concept relationship diagram for patient/person in health

It is also essential for a wider health environment to be able to ask other questions for each of physical and cognitive health, and for societal health. Understanding the relationships may lead to particular health policies (e.g. the role of immunization on a population).

5.3 Requirements on data and data processing

Data, when used in eHealth has to be explicable and transparent. This requirement can be addressed in part by ensuring proof of data provenance is available across all data processing points. For the use of data in Machine Learning (ML) or in AI the data sources will probably contain bias and this should be considered in interpretation of results.

EXAMPLE: Incidence of sickle cell anaemia is more common in certain demographic groups (particularly those of Afro-Caribbean descent) and much rarer, but present, in others. A dataset used in analysis of this illness that did not include all ethnic and demographic groups may make invalid inferences (e.g. assuming only those of Afro-Caribbean descent can suffer) and lead to unwarranted suffering by failure to recognize and treat the illness by demographic bias in the analysis and diagnosis.

The provisions for data explicability and transparency identified in ETSI GR SAI 007 [i.15] should apply in general to any use of data in eHealth.

6 Diagnostic eHealth use cases

6.1 Overview

The following actors are considered:

- Patient.
- Diagnostic sensor.
- Health professional (may be a machine (software or hardware or any combination thereof)).
- Context.
- Measurement metric standard.

The following statement is used to illustrate the use case:

- A <<Diagnostic sensor>> delivers a <<Measurement>> taken at <<time t>> in <<Context>> relating to <<Patient>> to <<Health professional>>.

There are additional statements to be made that apply to this use case:

- A <<Patient>> exists in a particular <<Context>>.
- A <<Diagnostic sensor>> complies with the specification for <<Measurement>> published by <<Publisher>>.

When related to the purpose of use cases outlined in clause 4.1 the following apply to diagnostic eHealth use cases:

What the problem is	Uncertainty in the cause of the medical complaint
Who has that problem (i.e. who will benefit when it is solved)	Patient
What are the consequences of the problem	Solution infers that the measurements, samples, and so on taken and analysed lead to a diagnosis identifying the cause of the medical complaint
What a possible solution would be, this sets the expectations and the scope of the solution (is it a new process, an application, etc.)	From symptoms, through analysis, to cause in order to identify a valid medical intervention to remove the medical problem

6.2 Data transfer

As identified in [i.3] data transfer requirements may be identified in an abstract form using a set of attributes that the date transfer scheme has to meet and which are presented and updated in Table 2.

Table 2: Data transfer attribute modelling (updated from ETSI TR 102 764 [i.3])

Attribute	Definition	Possible attributions
Ubiquity	A telecommunications or network service is considered as ubiquitous when it is, or seems to be, omnipresent within the scope of its deployment.	Yes No
Mobility	Mobility within a telecommunications network is used to refer to the ability of a device to change its physical point of attachment to the network without losing its logical connectivity. The obvious example is cellular radio where moving from one cell, the physical point of attachment, to another causes no interruption to the user service (the logical connection).	Infrastructure managed (e.g. cellular networking); End point managed (e.g. Local Area Wireless Networking); No mobility supported
Security	The security capabilities are selected from the CIA paradigm to counter risk to the system from a number of forms of cyber attack. The common model is to consider security in broad terms as determination of the triplet {threat, security-dimension, countermeasure} such that a triple such as {interception, confidentiality, encryption} is formed. The threat in this case being interception which risks the confidentiality of communication, and to which the recommended countermeasure is encryption.	Entity authentication; Infrastructure authentication; Cryptographic integrity generation and validation; Confidentiality provision (link encryption, end to end encryption); Service authorization; Key management
Connection capability	In telecommunications there are two distinct modes of operation, circuit mode and packet mode. A circuit mode call is often considered as traditional telephony where a simple definition may be that for the period of the communication there is a continuous electrical connection between the end points where the order of entry of data is preserved on exit. In practical terms there is not in fact an actual continuous electrical connection. Packet mode connections treat each packet as discrete and therefore it is possible that each packet takes a different route and thus may arrive out of order. The dominant mode in modern telecommunications is packet mode. The operational mode is distinct from the technology used to implement it, therefore traditional circuit mode services (e.g. voice calls) can be delivered using packet transmission capabilities (e.g. ATM, IP).	Packet mode - symmetric Packet mode - asymmetric Circuit mode - symmetric Circuit mode - asymmetric
Connection (address) topology	The topology of a connection is used to describe much of the physical connection of calls and covers three distinct cases. In each case a communications session may require a topology for each direction of connection.	Unicast (point to point); Multicast (point to multipoint); Broadcast (point to all points)
Content type	Whilst in a digital age all content can essentially be represented as a series of binary encoded information there are other characteristics that may be used to assist the ICT platform in carrying the content by syntactic and semantic labelling of content.	Data Video Audio (including speech) Image, deferred audio, deferred video, etc.
Grade of Service (GoS)	GoS refers to the ability to access and establish services and includes the time required to establish sessions, system reliability (assessment of Mean Time Before Failure (MTBF) and Meant Time To Repair (MTTR) for example) and recovery and system resilience (i.e. how it degrades).	Service establishment time System reliability System MTBF System MTTR
Quality of Service (QoS)	QoS refers to the maintenance of the session once established and covers aspects such as throughput, error recovery/detection.	Latency jitter end-to-end delay

6.3 Integrity and confidentiality

An observer of the system should not be able to determine the identity of the Patient or the Health Professional, nor make any assertion of the nature of the patient's health issue from observation of the content of the communication from the diagnostic sensor.

Any manipulation of the content of health data in the supply chain between the diagnostic sensor and the health professional should be visible to an observer.

6.4 Authenticity

The system should be able to unambiguously identify and verify the identity and function of the diagnostic sensor. The identifier and function should be able to identify the classification of the diagnostic equipment and the form of measurement it is delivering. Where a diagnostic measurement has to conform to a specific metric the system should retain a record of the calibration actions.

6.5 Non-clinical extensions of diagnostic eHealth

6.5.1 Contact tracing

The role of contact tracing in assisting a health professional in identifying who an infected patient has been in contact with, and who as a result may be at risk of having been infected, is a core component of containment of a contagion and is associated to a strict test and isolation protocol.

EXAMPLE 0: Any patient who has contracted HIV is often asked about their sexual history as their sexual partners may be at risk (the virus is spread by means including exchange of body fluids) and it is important to identify, test and protect each of them in order to protect the wider population.

NOTE 1: For very highly contagious cases where no test is available it can be necessary to isolate all of the population in the infected geo-region to restrict spread. The duration of such isolation strategies depends on a number of factors including the time before any at risk person will take to exhibit symptoms and the time taken for any recovering person to develop anti-bodies that may give a form of immunity to re-infection.

The contact tracing protocol is invoked on Alice being diagnosed with a transferable disease. The outline of the clinical protocol follows:

1) **Isolation:** Isolate Alice such that she is no longer able to transfer the disease to new contacts.

NOTE 2: Alice's isolation should normally be combined with treatment and should continue until such time as Alice is no longer symptomatic and unable to transfer the disease to anyone else.

NOTE 3: Whilst Alice is in isolation any medical professionals treating her should be protected in such a way that the risk of them becoming infected is minimized (e.g. by appropriate use of Personal Protective Equipment).

NOTE 4: Depending on the form of the contagion the way that Alice is isolated can vary.

2) **Contact identification:** Identify who Alice has been in contact with during the period prior to diagnosis and isolation where she has been able to transfer the disease to others (this determines Alice's list).

3) **Contact tracing:** The conventional approach to contact tracing is by interview of Alice by a designated health professional to get Alice to identify her movements and contacts. Technology may be used to supplement the contact information available from interview for certain modes of transfer.

EXAMPLE 1: Where a contagion is transferred from Alice to Bob by direct fluid transfer it is likely that Alice can directly identify all contacts that may be at risk.

EXAMPLE 2: Where a contagion is transferred in the air in Alice's expelled breath (aerosol transfer), and inhaled or absorbed from the air by Bob, it is unlikely that Alice will be able to accurately identify her contacts.

EXAMPLE 3: Where a contagion is transferred to a surface by contact it may be necessary to identify instances of Bob who have been at risk from transfer via the contaminated surface.

4) **Contact testing:** If Bob is identified as an at risk contact of Alice, then Bob is contacted for a diagnostic test. If Bob tests positive then Bob becomes a new root for the contact tracing protocol.

NOTE 5: Depending on the nature of the contagion, the time between contact and a true positive or negative test result, Bob may need to be tested multiple times.

6.5.2 Proximity based contact tracing

The normal, traditional role, of contact tracing is that Bob (from Alice's list) is approached by the health authority and asked to submit to a test. If Bob tests positive he will be asked to handover his contact list. Bob is then a new root for a new contact trace. Alice should appear on Bob's list but she will be flagged (by the health authority) as already tested and positive.

Constructing Alice's list for aerosol and contact transfer can be assisted by using device enabled proximity tracing. In such a scenario suitably equipped devices exchange identifying tokens if the conditions for proximity based contagion transfer are met. The content of the proximity based contact list should not be visible to Alice but may be transferred to a designated health professional by Alice, in particular it should be infeasible for Alice to determine the real identity of any instance of Bob that appears in the contact list.

The means by which Alice's list is made available to the health authority is outside the scope of the present document, however in order to be consistent with the generalized contact tracing protocol, the list should only be made available to the health authority after Alice has positively tested for the presence of a notifiable contagion.

NOTE: National governments have mostly agreed to maintain a list of notifiable disease, the criteria of which are maintained by the World Health Organization [i.12]. The legal frameworks for notification can be readily found and some examples are given below.

EXAMPLE: The UK protocol for notifiable disease recording is rooted in the Infectious Disease (Notification) Act 1889 [i.13] and extended since first coming into force. A weekly report of notifications is available online and linked from the UK government website [i.14].

Whilst outside the scope of the present document it is recognized that the means by which proximity contact lists are made available is the subject of significant debate. In broad outline Alice's list can be maintained centrally (always transferred to a central store), or locally (held on Alice's device). The argument between offline/local and centralized issue is both about privacy and processing time. In a centralized solution if Alice is tested positive and she has been sending her token to a central store then contact tracing is not dependent on Alice's response time, else it is.

6.5.3 Privacy concerns in proximity contact tracing

As indicated above it should be infeasible for Alice to determine the real identity of any instance of Bob that appears in the contact list. Similarly it should be infeasible for any unauthorized entity to view the content of Alice's list without both the presence of a verified positive test, and verification of Alice's consent to view the list.

If proximity detection devices include geo-fixed and located devices (e.g. a fixed Bluetooth enabled device) that is not associated to a human patient (i.e. there is no link between the device and any instance of Alice) the same broad requirements apply with the following exceptions.

A geo-fixed and located device is assumed not be directly testable, i.e. it cannot be associated with a positive test. If a cleaning or other sanitation regime identifies the presence of a communicable and notifiable disease in the proximity of the device the proximity contact tracing list of the device may be made available and be treated as if it had undergone a positive test (i.e. the contaminant was known or assumed to be active at the location of the device and at the time of contact). Similarly if the device is identified as being on Alice's list by the health authority the device's list should only be made available as a new root if a positive test can be associated to it.

7 Clinical intervention use cases

7.1 Overview

The presentation of use cases is similar to that used for diagnostic eHealth. The following actors are considered:

- Patient.
- Diagnostic sensor.
- Medical actuator.
- Health professional (may be a machine (software or hardware or any combination thereof)).
- Context.
- Measurement metric standard.

The following statement is used to illustrate the use case:

- A <<medical actuator>> delivers a <<stimulus>> at <<time t>> in <<Context>> relating to <<Patient>>.

There are additional statements to be made that apply to this use case:

- A <<Patient>> exists in a particular <<Context>>.
- A <<medical actuator>> complies with the specification for reaction to a <<Stimulus>> published by <<Publisher>>.
- A <<Diagnostic actuator>> acts only under command of a recognized health authority.
- A recognized health authority may be represented by suitably approved ICT equipment.

In general clinical intervention should follow a prescribed diagnostic and treatment strategy. Thus it is suggested that delivery of drugs or other clinical/medical treatment should be traceable to specific recommendations from the diagnostic analysis. The medical actuator and stimulus may be as simple as a timer based alarm informing a patient to take their medication, or be a more complex feedback loop such as an insulin pump which reads a patient's insulin levels and supplies insulin to ensure that "correct" insulin levels are maintained.

The following are forms of clinical intervention that may be augmented by eHealth technologies:

- Non-surgical intervention:
  - Drug monitoring and dose control:
    - In this use case the context refers to the set of diagnostic measurements that indicate that a stimulus is required, e.g. the measure of blood-sugar in the blood indicating a requirement for an injection of insulin to the blood.
  - Physical well-being control.
- Surgical intervention:
  - ICT assisted surgery:
    - In this use case the sensors and actuators required to perform surgery have to operate in real-time (or as close to as is practical), but decisions are made by a human operator. This conforms closely to the state of play today in which surgical procedures are made safe using eHealth technologies.

- ICT enabled surgery:
  - This extends the prior use case to address those parts of surgical intervention that may only be enabled by eHealth equipment. This conforms to many of the advanced keyhole and micro-surgeries that are enabled by eHealth technologies where unassisted and unenabled surgery would be impossible.
- Mechanical and ICT performed surgery:
  - This addresses the case where surgery is performed without direct human involvement.

When related to the purpose of use cases outlined in clause 4.1 the following apply to therapeutic eHealth use cases:

What the problem is	Provision of medical treatments in response to diagnosis of a medical complaint
Who has that problem i.e. who will benefit when it is solved	Patient, health professional
What are the consequences of the problem	For further study
What a possible solution would be, this sets the expectations and the scope of the solution (is it a new process, an application, etc.)	The therapy is applied

7.2 Ethical concerns

The provision of eHealth, wherein ICT devices act wholly or partly as agents of human health professionals, would be expected to ensure that the responsible party follows the general ethical frameworks that health professionals are expected to comply with, and to give assurance that devices "do no harm". See the World Medical Association International Code of Medical Ethics for obligations placed on medical professionals [i.4].

NOTE: Whilst not all health professionals are required to adhere to the WMA Code [i.4] the general assumption of most members of the public (as patients) is that the obligations apply to all and not only to physicians.

The use cases for clinical intervention need to at the very least ensure that there is an evidence trail to verify the provenance and validity of any healthcare action.

Where data is processed using AI or ML acting as a health professional or as an assistant to a health professional, the processing should be considered to be under the same ethical constraints as above. This will require that the AI/ML system is open to ethical review and its developers subject to liability constraints as for any other medical device or medical professional.

7.3 Non-clinical extensions of therapeutic eHealth

7.3.1 Contact tracing

As for clause 6.5 there is a role in therapeutic or clinical intervention for contact tracing. As noted in clause 6.5 contact tracing is an important part of the clinical protocol for test and intervention to limit the spread of contagions. The provisions of clause 6.5 apply.

8 Electronic Health records

8.1 Overview

8.1.0 Introduction

Diagnostic and preventative medicine requires access to a valid and accurate record of patient health over as long a period as possible. Thus whilst it may be argued that health devices (heart rate monitors, blood pressure monitors and so forth) are critical, they are only critical if the readings they take are recorded, and as is suggested in the use case statement, identify with some accuracy the context of the reading.

NOTE: Health records are required to cross international borders as has been explicitly stated in Directive 2011/24/EU [i.5] on patients' rights in cross-border healthcare. Whilst is it possible to conceive of a centralized supranational datastore maintained by a single data server, the security and reliability concerns of a single point of failure advise against it. Furthermore if such a centralized supranational server was to exist the political leverage afforded to the hosting country would be reasonably considered a significant source of risk to the operation of such a resource and thus advise against such a design.

8.1.1 Structure of a health record

A health record is a composite document and one of the difficulties surrounding the definition of a health record is in establishment of the boundary. In the domain of diagnostic medicine information is required to establish context. For example, many illnesses in their early stages have shared symptoms and to accurately attribute symptom to cause may mean the difference between survival and not.

A health record has no fixed start time and end time. Whilst for an individual a health record exists from birth, there are aspects of the individual's health that are directly linked to the parents (e.g. genetics) and to the period in the womb that need to be linked to the individual's record. Associated to the individual's record are also records of the health professionals, of the locations at which medical interventions occur (e.g. hospital, clinic), and of the medications prescribed, and so on.

8.2 What is the purpose of the records in eHealth?

A health record has a number of purposes, including but not restricted to the following:

- To log health status.
- To log health assessments.
- To log clinical interventions.
- To record recovery path.

A health record will also be used in review of the job performed by healthcare professionals and in specialist reviews such as reviews by Ethics boards, by transplant boards, by housing and social care agencies, by law courts and sentencing review boards and many more.

8.3 Access and Access Control

The concept of a health record as a composite document implies it may require different levels of access for each component of the document. Access control on anything that is not in the public domain should be based on a general principle of "need to know" or "least privilege". The problem in eHealth is that the details of who needs to know cannot be pre-determined so access control policies need to be flexible without harming the intent of minimizing exposure.

As a health record is not static, and is not a single element, but is required to be visible only to authorized entities steps should be taken to ensure that the entire set is protected from unauthorized access across its lifetime. In particular knowledge of one element of the record should not be able to infer the content of any other element of the record.

8.4 Cross border

The EU on behalf of all 27 member states has agreements that allow for the processing of data that is subject to GDPR [i.6] outside the borders of the EU-27. There is free movement of data internally to the EU-27 (e.g. any of the EU-27 states is allowed to store and process data in any of the other EU-27 states). eHealth data is subject to the provisions of the GDPR and should be processed in such a way that it maintains compliance at all times. This is in addition to the provisions stated in Directive 2011/24/EU [i.5].

NOTE: The member nations of the EU may change over time and it is recognized that EU rules, whilst binding on EU members, are also applicable to nation states that trade with the EU.

8.5 Security design considerations for health records

A health record has to have the following properties:

- the record is a collection of events or transactions related to a patient;
- the eHealth record is the collective term for the entire set of transactions;
- every transaction in the record has to have proof of the source;
- every transaction once entered into the record has to be considered as immutable and provably so.

The nature of a health record is that it is composed of many elements. The addition of an element can be considered to be discrete, and to be a timed event. If the health record is modelled as a distributed database of records then it may be possible to use a blockchain or distributed ledger approach to provide confidentiality protection of the growing record, or more conventional Merkle trees to protect the integrity of the growing record.

NOTE 1: A distributed ledger, often referred to as a blockchain, is a distributed database that maintains a continuously-growing list of records called blocks secured from tampering and revision. Each block contains a timestamp and a link to a previous block, in a Merkle tree like structure.

NOTE 2: A hash tree or Merkle tree is a tree in which every non-leaf node is labelled with the hash of the labels or values (in case of leaves) of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

Demonstrating that a leaf node is a part of the given hash tree requires processing an amount of data proportional to the logarithm of the number of nodes of the tree; this contrasts with hash lists, where the amount of processing required is proportional to the number of nodes in the list.

EXAMPLE 1: For a distributed health record consisting of 1 000 nodes or pages a hash tree can require several orders of magnitude less processing than a hash list.

The security design of linked data records should assess the role of trust in content and distribution. It is particularly of concern if a medical intervention or a precondition is not recorded that may have negative impact on the treatment offered.

EXAMPLE 2: If a person has an unrecorded, or unavailable, record of being (say) allergic to penicillin there is a significant risk that a treatment will be prescribed that triggers the allergic reaction which may result in a different, and negative, outcome from that intended.

9 Autonomic eHealth

The ultimate expression of eHealth is life-time health care without human intervention where the combination of sensors, diagnostic algorithms, and intervention actuators, give assurance of long term health.

Annex A:
Project UNCAP

A.1 Introduction

Ubiquitous iNteroperable Care for Ageing People (UNCAP) examined the role of technology in assisting the care of a very significant proportion of the global population. The percentage of the global population that is older than 65 years of age is growing, with many of the advanced industrial societies of the west already exceeding 20 % older than 65. If the general trend of industrial societies continues there will soon be significantly more than 1 billion individuals falling into this older people grouping. The matching trend is of a decreasing number of health professionals and over time it is reasonable to expect that there will be increasing need to provide medical care for the aging population by healthcare professionals increasingly distanced from the day-to-day experience of aging and the ailments that age confers.

To quote from the UNCAP press release:

"The ageing population is set to challenge health and care systems. Current care models are proving to be inappropriate and unsustainable. This situation is clearly calling for new care & assistance paradigms.

UNCAP will address such a fast-evolving scenario through the development of an infrastructure designed to ***help ageing people*** *(including those with* ***mild cognitive*** *impairments) live independently and with dignity.*

In particular, UNCAP will leverage on an interoperable ecosystem of biosensors and indoor & outdoor localisation solutions to deliver an infrastructure capable to continuously monitor and assist users in a non-invasive way.

Furthermore, UNCAP will allow accurate monitoring of user's state (physical & cognitive), and also creating a range of brand new services designed to stimulate ***healthier lifestyle*** *and more* ***active ageing process****. To this extent, the ultimate goal of UNCAP is to extend the duration of high-quality life of ageing, frail, and cognitive impaired citizens by helping them achieve higher* ***autonomy****,* ***independence,*** *and* ***dignity****."*

A.2 Use cases

A.2.0 Note about Use cases in UNCAP

NOTE: The uses cases in the UNCAP project have been developed as experimental scenarios, hence for example the "fall detection" use case has been examined to determine viability of various detection technologies.

A.2.1 Fall detection

A consequence of aging is, unfortunately, a greater likelihood to fall. Whilst the set of age related impairments that lead to this greater likelihood are of themselves not addressed in this use case the consequence of a fall often become more severe as one ages. Recognizing a fall as quickly as possible and making possible medical or nursing assistance as quickly as possible is the primary goal in this use case.

There are a number of ways that a fall can be detected:

- pressure sensors on the floor with processing of sensor data to distinguish a fall from walking or running, or even from sitting or laying down;
- visual recognition of a fall. In this case the motion of a person falling is quite distinct from other behaviours such as sitting or lying and a suitably equipped visual processing system should be able to identify a fall;
- body worn accelerometers may be used to detect a fall as there is distinct dynamic related to falling as opposed to normal sit down or lie down behaviour.

Monitoring a patient to determine he has fallen may be intrusive or subject to false alarms. There are a number of privacy issues too if the monitoring is pervasive. Thus the intent is to gather understanding of the viability of a number of non-intrusive fall detection systems, that preserve privacy and dignity as much as possible.

A.2.2 Medication reminder

Many mild cognitive disorders are characterized by mild memory loss (forgetfulness). Whilst the idea of technology to remind a person to take their medication is not complex of itself the aim in the experimental phase of the use case is to identify means that are relatively non-intrusive and that record the dosage taken - so more than a simple reminder that could be done by a simple alarm system - and reset for the next dose.

A.2.3 Exergaming

The purpose of exergaming is to provide a form of light-to-moderate physical activity for adults. To give medical feedback, particularly on the impact on cognitive performance, assessment of the physiological wellbeing as well as the psychological wellbeing has to be made. It has been suggested, and some evidence does exist, that exergames can improve mental, improve measures of physical performance, e.g. the narrow walk time test and self-reported balance confidence. In the UNCAP project data will be gathered to allow quantification of the results of supervised exergaming.

A.3 Healthy living

There is no good, well accepted, definition of a healthy lifestyle but good health probably requires both inclusion and avoidance in a reasonable balance. So in terms of diet is it reasonable to suggest that the diet is "balanced" between proteins, carbohydrates, fats and the rest. Similarly, it is commonly stated that being physically active is part of keeping healthy. The question that needs to be asked is "is the situation changing in a positive way?" In this respect the activity trackers (see Annex B) are of themselves not health devices as they do not track health status.

What is healthy? What is the starting datum point for assessing health? Is the lifestyle of the patient harming his health?

Annex B:
Fitness versus formal medical devices

A medical device is one that is classified as such and marked, in the EU, by an appropriate CE mark. Very simply a Medical Device (from Directive 2007/47/EC [i.2]) means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease;
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap;
- investigation, replacement or modification of the anatomy or of a physiological process;
- control of conception.

In addition to be considered as a medical device the object does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted by such means.

In contrast any other device, such as a fitness oriented Heart Rate Monitor (HRM), can only be used for indicative information and has to be specifically excluded from use in any form of diagnosis, monitoring, treatment or alleviation.

It is recognized that there are economic barriers to classifying a device as a medical device and devices that have medical or health value may not be formally classified as such.

EXAMPLE 1: A smartwatch in some variants may have a CE recognized function to identify and notify users of irregular heart rhythm that may be suggestive of Atrial Fibrillation (AF), but the same function may exist on smartwatches without CE recognition.

It is generally assumed that a fitness device will be internally consistent, i.e. its measurements will be consistent over time with itself even if inconsistent with other devices. Thus it may be reasonable to identify from a wellness device changes in behaviour that may indicate an underlying change in health.

EXAMPLE 2: A smartwatch with an HRM may record HR over continuous 24-hour periods and be able to determine trends in Resting Heart Rate (RHR). If the RHR drops or rises significantly over a period it may be indicative of a health issue that can notify the wearer to seek medical advice.

The present document does not distinguish between medical and fitness devices in general. The general statement that a <<Diagnostic sensor>> delivers a <<Measurement>> taken at <<time t>> in <<Context>> relating to <<Patient>> to <<Health professional>> holds with the variation that rather than delivering the measurement to a health professional, the fitness device may simply record the measurement of the sensor to the fitness record. It is less clear if wellness devices can be used in therapy even if many devices in the wellness sector are sold as therapeutic devices. In the examination of the generic use case in which a <<medical actuator>> delivers a <<stimulus>> at <<time t>> in <<Context>> relating to <<Patient>> a wellness device should only be considered in a health context if it can accurately record its activity, and, ideally, corelate it to a diagnosis based treatment advice.

Annex C:
Privacy considerations

Privacy in health care is a difficult topic and has close relationship to ethics and to dignity. Whilst ethics covers the questions of "is this the right thing to do?", "will this action lead to harm?", and dignity is a wider view of respect, the issue of privacy is more nuanced. There are many definitions of privacy but those from human rights regulation suggest that privacy is the "*right of the individual to have his identity, agency and action protected from any unwanted scrutiny and interference*". In healthcare it is often necessary for a lot of information to be gathered about lifestyle and actions to make a correct diagnosis and thus a correct treatment strategy. In a face-to-face conversation in closed room where there is a bond of trust between patient and doctor the patient may be more willing to disclose information that may otherwise be considered private.

NOTE: Privacy reinforces the individual's right to decisional autonomy and self-determination which are fundamental rights accorded to individuals within Europe.

The privacy concerns regarding eHealth are as a consequence of the loss of the closed room and the potential loss of the bond of trust established in a face-to-face conversation. The trust relationships established in pre-eHealth healthcare will not exist in the eHealth world in the same way.

Protecting patient privacy in eHealth is not as simple as simply encrypting files and file transfers. Privacy is rooted in both context and trust. Privacy protection has also to be considered alongside ethics, and alongside dignity. The former relates to being able to do the right thing at the right time, the latter relates to treatment of patients with respect and honour such that they maintain their dignity.

The core architecture of privacy protection has 3 elements as recognized in the GDPR [i.6]:

1) Data subject.

2) Data processor.

3) Data controller.

The data subject in eHealth is widely understood to be the patient but may also be a health practitioner, or indeed, any other actor in the system.

In addition it should be recognized that eHealth data is both private and of public concern.

EXAMPLE: A patient having a contagious or infectious ailment may be required to share that state with a health authority in order for public health actions to be taken.

Health data that is required to be shared to direct health policy or public health actions should be anonymized, i.e. it should be known that a patient exists in a particular location and time but it should not be possible to uniquely identify that patient without their informed consent.

The technical implications for privacy assurance are therefore not trivial. A single dataset may be concurrently used for patient treatment and for public health information, in the former case the patient and their health history may need to be exposed, whereas in the latter those elements of the dataset should be suppressed.

Annex D:
Extended glossary of terms

D.1 Introduction

Terms in common use in the Health domain often fail the requirements to be easily defined in an ETSI deliverable. The ETSI editing rules give the clear requirement that the form of a definition should be such that it can replace the term in context. Any additional information can only be given only in the form of examples or notes. This rather stringent rule makes a term, say health, difficult to simply define. When that same term is then extended by a modifier, such as eHealth, or mHealth, or telehealth, it becomes increasingly difficult to define with any degree of conciseness and still retain its accuracy. The purpose of this extended glossary is therefore to give a wider view of the meanings attributed to common terms in eHealth and to assist the reader in addressing the semantic, and syntactic meaning of a term.

D.2 Definitions and descriptions of eHealth domain

D.2.1 eHealth

The term "eHealth" is widely used by many individuals, academic institutions, professional bodies, and funding organizations in spite of there being no clear definition or understanding of its meaning. It can be considered as a generic term for the application of electronic Information and Communications Technology (ICT) across the whole range of functions that affect health. However this breadth of meaning is both a strength and a weakness. Saying eHealth will suggest to the recipient something about health and ICT but will not be able to specifically identify which health issue and which form of ICT.

Confusion surrounds the term and its presentation with multiple variants variously capitalized (e.g. eHEALTH, E-Health, e-Health) and hyphenated or not (e.g. eHealth, e-Health). Within ETSI the format eHEALTH referring to the ETSI Project has been preferred.

D.2.2 mHEALTH

Generic term for the application of mobile communications technology to the provision of health care services.

NOTE: Insofar as mHEALTH and eHEALTH have merged the primary difference in meaning is with the role of the terminal device connection to the network. It may be considered that mHEALTH is a subset of generic eHEALTH for connectivity of the end-points making use of cellular network technology. The existence of wireless (radio) technology to connect a sensor to a hub or processor does not imply mHEALTH.

D.2.3 Telemedicine

Integrated ICT environment designed to provide healthcare services by use of a remote internet connection between the patient and a medical practitioner, offering patients express diagnostics and advice outside medical facilities and conventional clinic hours.

D.2.4 Telecare

Remote healthcare involving patient monitoring.

D.2.5 tele-health

Tele-health includes surveillance, health promotion and public health functions. It is broader in definition than tele-medicine as it includes computer-assisted telecommunications to support management, surveillance, literature and access to medical knowledge.

D.3 Definitions and descriptions of eHealth actors and services

D.3.1 Telematics for health

Telematics for health is a WHO composite term for both tele-medicine and tele-health, or any health-related activities carried out over distance by means of information communication technologies.

D.3.2 Health Care Professional

The definition of health care professional is a superset of that of Health Care Provider (given below) in that there is as assumption of a governing body for and that the individual is paid for providing care.

D.3.3 Health Care Provider

A doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC [i.11], or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC [i.11], or a person considered to be a health professional according to the legislation of the Member State of treatment.

Article 3f) of Directive 2011/24/EU [i.5] on the application of patients' rights in cross-border healthcare.

Annex E: Bibliography

- ETSI SR 002 564: "Applicability of existing ETSI and ETSI/3GPP deliverables to eHealth".
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

NOTE: Available from https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
- ETSI TS 103 264 (V2.1.1) (03-2017): "SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping".

History

Document history		
V1.1.1	October 2019	Publication
V1.2.1	August 2020	Publication
V1.3.1	January 2023	Publication