(one6G)

Taking communications
to the next level

6G AND EHEALTH: USE CASES AND POTENTIAL SERVICE REQUIREMENTS VOL. 2

WHITE PAPER

September 2026

one6g.org

Contributors

Institute	Person	Section
King's College London	Thomas Booth, Xingyu Chen, Mohammad Shikh-Bahaei, Emmanouil Spyrakos-Papastavridis	Section 4
	Mona Ghassemian	Section 5
University of Stellenboch	Dirk Brand *1	Section 5
Klinix	Segun Bello	Section 5
University of Nevada	Lee Barford	Section 5
NIST	Kamran Sayrafian *1	Section 5
Université Catholique de Louvain	Mohsen Shirali *2	Section 5
UniFi	Lorenzo Mucchi	Section 5, Section 4
SmartAvatar B.V.	Albena Mihovska	Section 4
Huawei	Onur Ayan, Joseph Eichinger, Markus Dillinger, Ramya Panthangi Manjunath	Section 4

*1 Guest Contributor

*2 Author contributed to the white paper while affiliated to the corresponding institute

Change history

Date	Update	Person
27/07/2026	First draft of eHealth white paper – vol. 2	Ramya Panthangi Manjunath
10/08/2026	Second draft of eHealth white paper – vol. 2 • Updated new use case description • Updated Section 4 • Updated contributors • Drafted conclusion • Update the list of contributors	
14/08/2026	Third draft of eHealth white paper – vol. 2 • Updated Scope • Updated Definition of Terms • Updated use case requirements • Update section: The Multistakeholder eHealth Ecosystem • Updated conclusion • Updated references and abbreviations	
19/08/2026	Fourth draft of eHealth white paper – vol. 2 • Updated Introduction • Updated the use case description section with a short concluding section • Updated conclusion and next steps • Some editorial formatting • Addressed received comments	
19/08/2026	Fifth draft of eHealth white paper – vol. 2 • Updated Telesurgery use case	
25/08/2026	Sixth draft of eHealth white paper – vol. 2 • Updated figures for some use cases • Cross-checked the references	

Scope

One6G has identified eHealth as one of the promising domains where mobile communication systems can help. Given that 6G is envisioned with capabilities beyond connectivity—such as sensing, localization, and environmental and health status awareness—eHealth represents a potential domain where these innovations can complement, enhance, or expand healthcare and healthcare management systems. In particular preventive medicine must be supported by 6G systems. 6G health systems should support professional medical services and devices e.g., in hospitals but also health devices which are in the responsibility of consumers (e.g., smart watches). Different regulations govern these 2 categories.

The previous release of one6G eHealth white paper titled “One6G Vertical Use cases” [1] and “6G & eHealth: Use Cases and Potential Service Requirements” [2] identified several use cases and analysed system requirements (from functional and key performance indicators perspective) for both connectivity and beyond-connectivity capabilities envisioned for 6G mobile networks. These works highlighted that 6G capabilities, including highly accurate sensing, localization, reliable connectivity, advanced in-network computation, and AI are critical enablers for next-generation healthcare services, particularly in addressing challenges like aging populations, rising costs, and staff shortages.

Building upon the foundational work presented in the first volume of the one6G eHealth white paper [2], the scope of the second volume is extended in the following key directions:

- Survey of eHealth related used cases in 6G standard development organizations (e.g., 3GPP, ETSI).
- Identification of potential new use cases and requirements.
- Comprehensive analysis of cross-domain standards and regulations, encompassing medical device standards, ethical frameworks, security protocols, and data privacy.

This volume of the white paper aims to take a step towards developing a holistic understanding of the eHealth ecosystem—encompassing its clinical, operational, and regulatory dimensions—with primary focus on how mobile communication networks can serve as a valuable stakeholder within this broader system. By offering connectivity and beyond-connectivity services such as sensing, AI/ML, and compute services, mobile networks are positioned as active enablers of several eHealth use cases such as remote monitoring, AI-driven diagnostics, and secure data exchange platform across care settings. Their design must therefore address the stringent demands of healthcare, including privacy, cybersecurity, regulatory compliance, ethical AI, and patient safety. While regulatory baselines are essential, long-term adoption will ultimately depend on fostering user confidence through transparent, human-centric design that preserves patient trust.

Table of Contents

1. Definition of terms

In addition to the definitions of terms related to wireless communication, wireless sensing, and AI/ML support services already established in previous release of one6G eHealth white paper [2], this volume introduces and defines a new set of terms. These additional definitions extend the existing vocabulary to cover emerging concepts and novel system architectures relevant to the evolving eHealth domain.

AI related terms and definitions

- **6G AI Service:** a service provided by the 6th Generation (6G) network where AI functionalities (e.g. AI model training, AI model management or AI inference) are made available to a subscriber/user or an authorised application on the User Equipment (UE) or on an application server (AS) [4].
- **6G Computing Service:** a service provided by 6G network utilising computing resources in Service Hosting Environment, which can be used by a subscriber (via UE)/3rd party [4].
- **Service Hosting Environment:** the environment, located inside of 6G network and fully controlled by the operator, where Hosted Services are offered from [4].

Agents related terms and definitions

- **AI Agent:** an automated intelligent entity that achieves a specific goal (autonomously or not) on behalf of another entity, by e.g., interacting with its environment, acquiring contextual information, reasoning, self-learning, decision-making, executing tasks (independently or in collaboration with other AI Agents) [4].
- **Intent:** expectations including requirements, goals and constraints without specifying how to achieve them [4].

2. Introduction

The eHealth domain represents a broad and multifaceted intersection of healthcare, information technology, and data science. It encompassing everything from electronic health records and clinical decision support to patient portals and population health analytics. However, the focus of this section narrows specifically to the telecommunication-related activities that form the critical backbone of modern digital health.

The healthcare sector has emerged as a critical vertical for standardization efforts in 3rd Generation Partnership Project (3GPP) and ETSI. These organizations are actively engaged in gathering requirements and developing technical specifications to enable a wide spectrum of eHealth applications. Currently the mobile communication industry is laying the groundwork for future 6G systems. By capturing requirements early in the standardization process, technology development can be guided in a direction that is genuinely beneficial from the very beginning.

The 3GPP has been actively discussing several healthcare-related use cases in its latest Technical Report on 6G use cases [3]. Specifically, there are seven distinct use cases spanning from personalized AI health monitoring and home robots to holographic telepresence and mission critical services. In addition to sensing and positioning services from the networks, these healthcare use cases have highlighted several key requirements, including the offloading of computing tasks from a UE to the 6G network, secure communication among AI agent applications, collaborative operation of AI agents across multiple UEs, support for AI agents to access 3GPP services, highly reliable holographic telepresence, and energy-efficient transmissions from devices running on a 3.3V battery with a capacity under 1000 mAh. These represent some of the identified requirements.

In light of the growing interest in integrated sensing and communication (ISAC) functionalities within 6G networks, ETSI has published a report on ISAC use cases [3] where several health-related use cases are examined. The four use cases address motion recognition (macro and micro), proximity-based fall detection, outdoor emergency monitoring, and robotic senior care—each with distinct sensing and fusion challenges. It is expected that the 6G system can simultaneously recognize multiple types of large-scale (e.g., walking) and small-scale (e.g., breath rate, hand gestures) motions, and distinguish between human body and non-human object based on received sensing signals. Additionally, sensing is expected to operate as desired in both indoor and outdoor environments such that the transmission power remains within the regulatory limits. Furthermore, user consent and adherence to regulations is essential for sensing data.

In addition to requirements and the corresponding communication technology development activities, the 3GPP SA3 working group [4] is studying security architecture, RAN security, UE to core network security, subscription authentication and authorization, security and privacy aspects of network exposure, data framework security, and sensing security and privacy, among others. This expansion is particularly critical for healthcare and human-centric sensing use cases, where the fusion of sensitive biometric and location data necessitates robust, end-to-end privacy guarantees that go beyond traditional communication security.

Driven by the current standardization activities, the contribution of this white paper is twofold. First, through a comprehensive use case analysis, identify new requirements that are not currently being captured in existing standardization efforts. Second, this white paper draws much-needed attention to the broader eHealth multistakeholder ecosystem—spanning patients, healthcare providers, technology vendors, regulators, and policymakers. This ecosystem is governed by a complex web of interrelated standards covering not only security and privacy, but also patient safety, data integrity, interoperability, and ethical considerations. Navigating this landscape requires a coordinated approach that balances technical robustness with regulatory compliance and ethical responsibility.

3. Methodology for use case description and analysis

Following the methodology introduced in the previous volume of the white paper [2], the use cases presented in this white paper also largely follows the template used by 3GPP to potential new requirements that would be needed by the 6G system to realize them. The 3GPP template follows the three-stage standardization method as outlined in ITU-T Recommendation I.130. An overview of each section of the use case template is provided below for reference.

This volume organizes its use cases around the same use case clusters considered in the previous volume of the white paper [2]. Additionally, a few new clusters are identified. In the following the new clusters are described.

Agentic AI health monitoring

6G systems are foreseen to natively integrate sensing, communication, and computation, enabling the deployment of autonomous AI agents that can perceive, decide, and act in real time. In healthcare, these agents will interface with wearables such as smartwatches, biosensors, and glucose monitors to continuously collect and process patient data, detect anomalies, and trigger timely alerts or interventions. Leveraging ultra-low latency and high reliability, 6G-enabled agents can support proactive, personalized care—for example, predicting cardiac events or managing chronic conditions—while seamlessly coordinating with healthcare providers and emergency services.

Smart Body Area Network

ETSI SmartBAN and 3GPP network integration enables seamless communication between wearable body sensors and cellular infrastructure, unlocking advanced healthcare use cases. SmartBAN provides short-range, low-power connectivity for continuous monitoring of vital signs—such as heart rate, blood pressure, and glucose levels—from on-body sensors. Through integration with 3GPP 6G systems, the collected data is securely transmitted over mobile networks to healthcare providers in real time. This convergence supports remote patient monitoring, fall detection, post-surgical tracking, and emergency alerting, leveraging 3GPP's low-latency, high-reliability capabilities alongside SmartBAN's energy-efficient operation.

AI-enabled mobile network for healthcare applications

AI-enabled mobile networks embed AI/ML models directly within the network infrastructure—at the RAN, edge, and core layers—to deliver intelligent, low-latency healthcare services. By fusing multi-modal data streams from wearables, environmental sensors, and user location, these network-resident AI capabilities enable real-time monitoring, anomaly detection, and adaptive interventions. For instance, they can process sensor data to provide navigation assistance for people with disabilities, such as guiding visually impaired users while detecting obstacles. Similarly, network-resident AI can analyze mobility patterns and symptom reports to generate early public health alerts and identify outbreak hotspots. Leveraging the distributed computing

fabric of 6G, these AI engines ensure timely, privacy-aware, and scalable healthcare delivery across diverse care settings.

By aligning to what 3GPP is currently studying and discussing, we make sure that the use case clusters in this paper are relevant to ongoing standardization work that will shape future 6G systems.

For ease of reference, the use case description template is reproduced below from [R].

Description

Short description of the use case. A couple of paragraphs that defines the background (e.g., necessity), context (e.g., human-in-the-loop) and environment (e.g., nursing ward) of the use case.

Pre-conditions

Necessary capability of the different actors to ensure the realization of the use case.

Service Flows

The flow of events from the moment the use cases is triggered to the moment the use case closes. Each step is an action from an actor (e.g., doctor or 3GPP entity). One or two sentences per step.

Post-conditions

Output or outcome once all steps in the service flow have occurred. One or two sentences to describe post-condition.

Existing features/requirements covering the use case

Identify existing features in current 5G/5G-A system that partially or fully cover required use case functionality. Slightly differing from the original 3GPP template and the template used in previous volume of the whitepaper, this section additionally outlines the existing 6G service requirements from [4] that are partially or fully applicable to the use case. The discussion of existing features or requirements is grounded in what could be ascertained for the use case.

Potential new requirements needed to support the use case

- Identify new functionality that future 6G system should have to enable use case
- Functional requirements
- Operational requirements

Key Performance Indicators

Key Performance Indicators (KPIs) that need to be satisfied to enable the user story defined for the use case.

- e.g., More stringent KPIs in terms of communication (including AI/ML support) and sensing

4. eHealth use cases and requirements

With 3GPP 6G service requirements [4] serving as the baseline document, our objective is to identify any emerging requirements that are not yet addressed in the current specification.

4.1 Wireless sensing

4.1.1 Real-time equipment and status tracking

1. Description

The goal of the use case is to enable real-time tracking of different medical equipment's within a hospital and care centers. Equipment refers to assets and devices (e.g., e.g., thermometers, portable ultrasound, hospital beds, AED, wheelchairs, etc) and consumables (e.g., medicines, catheter, etc) that are utilized for the patients. According to findings in [5], more than one-third of the nurses spend at least an hour finding items of equipment during an average hospital shift. This amounts to significant number of hours being spent on searching equipment which could otherwise be utilized for patient care.

Enabling real-time tracking of medical equipment can result in reducing the search time for nurses, minimizing the delay in patient care, and potentially avoiding excessive ordering of different equipment thereby reducing costs.

Implementing real-time equipment tracking requires several challenges to be addressed. Some of them include identification of large number of equipment, counting the number of equipment, dynamically mapping the identified equipment to the appropriate location within the hospital, attaching 6G RFID tags to small scale items, identifying the status of the assets, and integrating all the asset information into the existing inventory management system.

An overview of the use case is illustrated below:

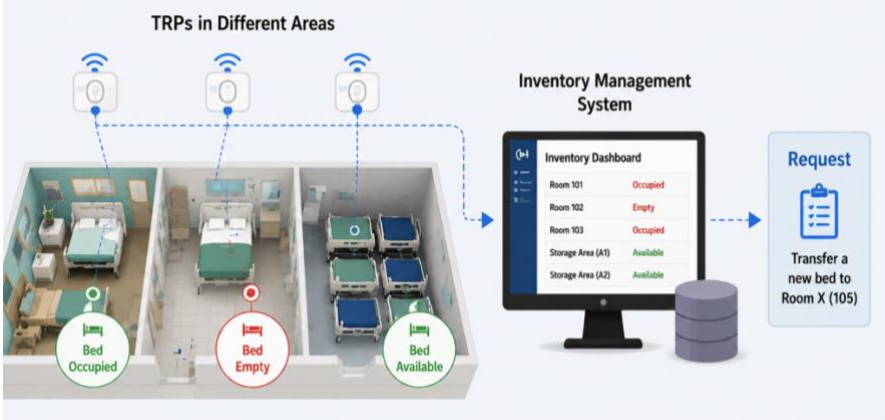

Figure 1: Illustration of ISAC based asset tracking use case [AI generated image].

2. Pre-conditions

The equipment to be tracked are identified. Different equipment is clearly labelled to enable tracking. The different rooms within in the hospitals are identified. An inventory management system primarily comprising of a database hosted either in the hospital premises or by a third-party hospital inventory management system.

Transmit Receive Points (TRPs) are small indoor base stations or distributed antenna system with the capability to perform 3GPP sensing (acting as sensing transmitter and sensing receiver). These are fixed at different location in the hospital on the roof. The hospital has agreement with the owner of the TRP to perform 3GPP sensing and share the result to inventory management system. Each medical personnel have access to the current inventory status from the inventory management system via display units at multiple locations in the hospital.

3. Service Flows

An example service flow is described below:

1. The TRPs located in different parts of the hospital continuously sense the different assets along with their status. This information is henceforth referred to as sensing results. An example of an asset along with its status includes empty beds.
2. The sensing result is transmitted to the inventory management system.
3. A healthcare personnel receives a request to transfer a new bed to room *X*.
4. The healthcare personnel access the inventory status in the inventory management system to identify the location of the required asset.
5. The healthcare personnel directly collects the asset from the indicated location.
6. The healthcare personnel transfers the requested asset to the desired room.

4. Post-conditions

The assets are efficiently utilized. The healthcare personnel are more productive. The assets are continuously tracked and their status is stored in the database.

5. Existing features/requirements partly or fully covering the use case functionality

Some of the requirements partly covering the use case include:

- Subject to operator's policy, the 6G Network shall provide sensing service to detect, classify and count one or more sensing targets.
- The 6G network shall be able to provide a means to securely expose the feasibility to deliver the sensing result within delivery time window, as requested by an authorised 3rd party.
- Subject to operator's policy, regulatory requirements and subscriber permission, 6G network shall support the ability to derive a sensing result based on the stored sensing data and ensure that only authorised entities are able to access sensing results.
- Subject to operator's policy and regulatory requirements, the 6G system shall provide a sensing service to predict the characteristics of sensing targets (e.g. shape and size of the vehicle).

6. Potential new requirements needed to support the use-case

[PR1] The 6G network shall provide sensing service to determine the state of a sensing target. For example, if the sensing target is beds in the hospital, the sensing system is able to determine if the bed is in use or available.

[PR2] The 6G network shall enable configuration of user-defined states for sensing targets.

[PR3] The 6G network shall ensure that the sensing operations comply with privacy regulations by protecting individual identities during the collection, processing, and reporting of sensing results. (E.g., any sensitive information about the individuals around the sensing target, such as an empty bed, should not be exposed).

7. Key Performance Indicators

Some relevant KPIs include:

- Positioning accuracy depending on the asset type and its size.
- Missed detection probability needs to be low.
- False alarm probability needs to be low.

4.1.2 Outdoor On-Demand Sensing: Safety & Wellness

1. Description

Individuals in outdoor environments could sometimes encounter emergencies. Emergencies requiring prompt response typically relate to public safety and/or healthcare. Timely help in such unanticipated scenarios could be decisive between survival and fatal outcomes. This use case is about utilizing sensing-capability of mobile networks to aid individuals in case of outdoor emergencies. The sensing-capability from the mobile network can monitor the individual and his/her surrounding as per the individual's needs, and directly trigger the emergency response in case of a detected event. The trigger to initiate and terminate network-based sensing for emergency purpose is dependent on the individual. Sensing includes capturing 3D positions and related trajectory of individuals. Existing 5G Advanced positioning techniques will be improved and augmented by 6G ISAC to increase accuracies.

The table below includes a list of scenarios where this use case is applicable.

Scenario	Example
Healthcare related	In situations where the user wants to be monitored while exercising outdoors, or for seniors who need fall detection that triggers an immediate response from healthcare providers.
Public-safety related	In situations when user feels vulnerable and need a prompt police connection while walking through deserted or dimly lit streets.

An overview of the use case is illustrated below:

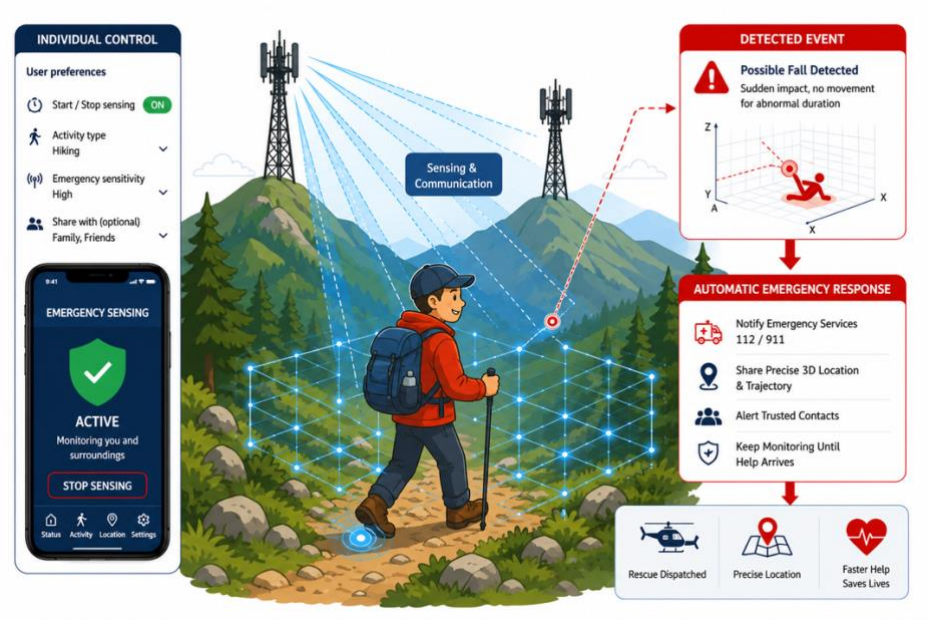

Figure 2: Illustration of outdoor on-demand sensing use case [AI generated image].

2. Pre-condition

- The base stations supporting the sensing service are configured with 3GPP-compliant integrated sensing and communication.

- The 3GPP network (including the location management function (LMF) and access network) is provisioned to provide positioning capabilities (e.g., RAT-dependent and RAT-independent positioning methods) supporting the required accuracy, latency, and coverage for the sensing service.
- The user (or application acting on behalf of the user) is authorised to request the start and termination of the 3GPP sensing service at will, subject to network policy, user subscription, and applicable regulatory constraints.
- Service-level agreement exists between the mobile network operator (MNO) / base station owner and the authorised law enforcement and healthcare responder entities.
- Application server (within the network or a 3rd party service provider) receives sensing data to process the user request.

3. Service Flows

An example service flow is described below:

1. User A wants to go jogging in a park.
2. User A opens an application to request 3GPP sensing service from the mobile network. The sensing request comprises of, among other aspects, the approximate route of the jogging path, approximate jogging duration, individual sensing criteria (e.g., fall detection, inactive detection, constant real-time monitoring of surrounding within 50m range to detect suspicious behaviour (e.g., follower)).
3. The mobile network determines if the desired sensing requirements from the user can be fulfilled and notifies the availability of the sensing service to the user via the application.
4. User A starts jogging. User A decides to rest on a bench after sometime. User A is inactive and is resting for a usually long time.
5. The mobile network receives an indication of User A's inactivity from the application server.
6. The mobile network triggers emergency response via a notification or sharing the live sensing stream.
7. User A/emergency response terminates the sensing service when recovered or located by the emergency response personnel.

4. Post-conditions

User A was continuously monitored as desired. User A promptly received help from healthcare personnel. The mobile network initiates and terminates sensing based on demand.

5. Existing features/requirements partly or fully covering the use case functionality

Some of the requirements partly covering the use case include (in addition to Section 4.1.1):

- Subject to operator's policy, regulatory requirements, the 6G network shall be able to provide sensing results to a UE or an application on a UE, where the UE is authorised by the network operator to use the sensing result for a specific service (e.g. to combine sensing result).

- Subject to operator's policy, regulatory requirements, the 6G network shall be able to provide a sensing service that is able to derive predicted location and/or velocity of sensing target(s) as requested by a subscriber or an authorised 3rd party.

  Subject to operator's policy, regulatory requirements, the 6G network shall be able to provide secure means to expose the prediction of location and/or velocity of sensing target(s) to an authorised 3rd party.

6. Potential new requirements needed to support the use-case

[PR1] The 6G system shall be able to enable and disable the sensing service when triggered by an application on the UE.

[PR2] The 6G system shall be able to link sensing results and positioning results to improve positioning accuracy.

[PR3] The 6G system shall be able to ensure privacy of individuals while sensing and generating sensing result.

[PR4] The 6G system shall support the capability to enable sensing service to trigger a third-party application servicer to initiate an authorization procedure and subsequently share the sensing result or live sensing stream.

[PR5] The 6G system shall support the termination of the serving service from user authorized entities or applications from another UE.

7. Key Performance Indicators

Some relevant KPI includes:

- Sensing service area is outdoor
- Sensing accuracy (positioning and velocity accuracy) and sensing resolution is subject to sensing target.
- Expected beyond communication latency: <20s for identification of alarm and notification generation.
    - Note: Based on the time taken to answer emergency calls in 23 EU member states on an average, which is less than 10s [6]. Considering additional 10s to identify the emergency and notify the appropriate response team.

4.2 Agentic AI health monitoring

4.2.1 AI Agents based health monitoring

1. Description

Wearable health, brain and body monitoring devices are being widely adopted across diverse populations. These devices have evolved from capturing simple metrics such as steps count to more sophisticated physiological and biochemical metrics such as heart rhythm, sleep tracking, and blood oxygen saturation, among others. Such devices are developed by several manufacturers and offer several features beyond simple data sharing among the authorized persons (e.g., family members, caretakers). In the future we expect non-invasive and invasive sensors and actuators which are used for health purposes and as serving new human-machine interfaces (HMIs). As an example, are the recent advances from Brain-Computer-Interface (BCI) research activities connecting body implants (non-invasive/invasive). 6G can be the wireless bi-directional BCI in the future.

The goal of this use case is to complement the features of existing health monitoring and future wearables (body, implants) with capabilities offered by 6G mobile networks. The mobile network could offer a unified platform to seamlessly integrate sensing data from multiple sources (e.g., wearables, cameras, network-based sensing), provide timely health-related insights using AI, and dynamically adapt the offered features such as history duration for data analysis (for specific metrics), geofencing, and threshold to trigger alerts, among others. Beyond combing and analyzing health, brain and body data, the network can enable changing monitored metrics and/or data-sharing ecosystem based on demand and authorization. In principle, the 6G network can behave as an integrated dashboard for multiple users to monitor, analyze, trigger alerts, and share heath related data seamlessly to enable prompt actions.

6G network could enable such scenarios by supporting and integrating AI agents within its infrastructure. The network and the user equipment (UE) are considered to host AI agents. These AI agents are expected to act based on the received intent. In one example, the user (e.g., patient) or a UE (i.e., on-device) AI agent may provide an intent and express its consent (after necessary authentication measures have been applied) via its 6G-capable device to the network. An example intent is to monitor a set of the person's health metrics from one or more mentioned devices and report to desired party in case of any deviations. The Network AI Agents are required to parse the request, setup necessary connectivity services proactively among the different AI agents, so that the UE AI agents are able to transmit in a reliable and timely manner, when required. When the UE/Network AI agent detects an anomaly that exceeds its local diagnostic confidence threshold, they dynamically initiate collaboration for the next actions.

2. Pre-conditions

- A user possesses a health monitoring device (UE) equipped with AI agents to collect real time biometric data, e.g., hear rate, oxygen saturation, body temperature, etc.
- The UE hosting the on-device AI Agent is authorized, authenticated, and attached to the PLMN.
- The 3GPP system supports an AI Agent identity framework, enabling mutual authentication and secure communication between the UE AI Agent and the Network AI Agent.
- The user has provided explicit, verifiable consent for the collection, transmission, and processing of sensitive biometric and positioning data by the Network AI Agent.
- The Network AI Agent has securely registered its analytical services and capabilities with the network framework, making it discoverable for the on-device AI Agent.

3. Service Flows

1. The on-device AI Agent queries the network to discover an appropriate Network AI Agent capable of health data processing and establishes a secure, end-to-end encrypted communication channel.
2. The on-device AI Agent continuously collects biometric and environmental data. It performs lightweight local filtering to preserve battery life and securely streams the relevant telemetry to the Network AI Agent over the access network.
3. The Network AI Agent utilizes in-network computing resources to run large-scale AI/ML inference on the incoming data streams, correlating it with user-specific historical health parameters.
4. The Network AI Agent detects a critical deviation in the user's health metrics.
5. The Network AI Agent autonomously formulates an "emergency intent" and securely exposes the processed anomaly data.
6. Recognizing the emergency, the Network AI Agent dispatches an emergency request to 3rd party medical services in the user’s service area and provides precise location information and description of the user’s emergency condition.

4. Post-conditions

- Timely and context-aware medical assistance reaches the user based on the efficient multi-agent collaboration.
- The anomaly logs are securely archived (after anonymizing the data to ensure user privacy) to refine and train future AI/ML models via federated learning.

5. Existing features/requirements partly or fully covering the use case functionality

Some of the requirements partly or fully covering the use case functionality [4]:

- Subject to operator's policy, the 6G network shall support mechanism (e.g. AI capabilities such as AI Agent) to provide suitable 3GPP service or combination of multiple 3GPP services in response to received request for service (e.g. expressed via Intent(s)) from subscriber/users, or an authorised 3rd party.
- Subject to operator's policy, regulatory requirements and subscriber permission, the 6G system shall support mechanisms (e.g. AI capabilities such as AI Agent) to translate Intent received (e.g. from subscribers/ users) into 3GPP services and service performance requirements.

- Subject to operator's policy, regulatory requirements and subscriber permission, the 6G system shall provide a suitable means for an authorised AI application (e.g. 3rd party AI Agent) to request 3GPP services (e.g. AI service).
- Subject to operator's policy, regulatory requirements and subscriber permission, the 6G network shall support a mechanism to authenticate and authorise an AI application (e.g. 3rd party AI Agent) requesting 3GPP service.
- Subject to operators' policy, regulatory requirements and subscriber permission, 6G system shall support communication service (e.g. including multi-modality data exchange) among authorised AI applications (e.g. 3rd party AI Agents belonging to the same or different users) via the 6G network.

6. Potential New Requirements needed to support the use case

[PR 1] Subject to operator's policy, regulatory requirements and subscriber permission, the 6G system shall support mechanisms (e.g. AI capabilities such as AI Agent) to translate Intent received (e.g. from subscribers/ users) into 3GPP services requirements and actions for intent handling.

[PR 2] The 3GPP system shall provide mechanisms to enforce strict end-to-end data privacy, ensuring user consent is collected and verified before any local biometric data is exposed to Network or 3rd-party AI Agents.

[PR 3] The 3GPP system shall support secure authentication, authorization, and discovery mechanisms for on-device AI Agents, Network AI Agents, and 3rd-party AI Agents based on unique digital identities.

[PR 4] The 3GPP system shall support a standardized framework for the Network AI Agent to securely expose synthesized network data (e.g., high-precision positioning) and processed intelligence to authorized 3rd-party application agents.

4.3 Smart Body Area Network

4.3.1 Continuous Wearable Health Monitoring through ETSI SmartBAN and 6G

1. Description

ETSI SmartBAN is a standardized framework developed by the ETSI Technical Committee SmartBody Area Network for communication and interoperability among low-power devices located on, around, or in proximity to the human body. Its specifications address low-complexity and ultra-low-power physical and medium-access-control layers, as well as relay and hub-to-hub communication, data representation, and semantic interoperability. SmartBAN is particularly relevant to health and wellness applications involving wearable or personal sensing devices.

An example scenario connecting 6G and SmartBAN is as follows: a patient at home wears smartBAN sensors that continuously track his vital signs like heart rate and oxygen saturation, among others. These sensors send the data to a nearby hub which forwards it to the healthcare service via 6G network. Clinicians can then remotely monitor the patient's conditions allowing for quick response. The remainder of this section delve deeper into this scenario.

2. Pre-conditions

- A patient wears multiple low-power sensors for periodically or continuously measuring physiological and activity-related parameters, such as heart rate, oxygen saturation, body temperature, respiration, posture, and movement.
- The sensors form a Smart Body Area Network and communicate with a SmartBAN hub, which may be integrated into a smartphone, wearable gateway, or dedicated medical device.
- The SmartBAN hub forwards sensor data to a Smart Coordinator which bridges the SmartBAN hub traffic towards external infrastructure.

3. Service Flows

An example service flow is presented below:

1. Upon returning home after his operation, Bob's physiological and activity data must be monitored for a few days without interruption, even as he moves freely between indoor and outdoor spaces.
2. The SmartBAN sensors around his body continuously transmit measurements to the SmartBAN hub.
3. The hub collects and preprocesses the sensor data. The preprocessing includes data aggregation, quality assessment, and preliminary event detection.
4. The preprocessed data at the SmartBAN hub is forwarded to the Smart Coordinator.
5. The Smart Coordinator transfers routine data and emergency alerts towards the healthcare service through the 6G infrastructure.
6. Upon detecting an alert, prompt action by healthcare professional is triggered.

3.4. Post-conditions

Bob was continuously monitored for a few days. The measurements from SmartBAN sensor network were transmitted over the 6G network to the healthcare service without interruptions as per the monitoring schedule.

3.5. Existing features/requirements partly or fully covering the use case functionality

Current 5G and 5G-Advanced systems provide several capabilities that partly support this use case, including differentiated QoS, mobility and session continuity, network slicing, edge computing, network capability exposure, authentication, and communication security. In addition, 3GPP TS 23.542 provides application-layer support for Personal IoT Networks.

On the SmartBAN side, [7] introduces the Smart Coordinator as the entity responsible for coordinating SmartBAN hubs and bridging SmartBAN traffic towards external infrastructures. However, standardized interworking between the Smart Coordinator and 3GPP systems, including the mapping of SmartBAN-specific data, metadata, traffic priorities, and security requirements, is not yet fully defined.

3.6. Potential new requirements needed to support the use case

[PR 1] The 6G system shall support standardized interworking with the ETSI SmartBAN Smart Coordinator, enabling authorized transmission of SmartBAN data and associated metadata towards healthcare services.

[PR 2] The 6G system shall support the mapping of SmartBAN traffic priorities and QoS requirements to appropriate communication and computing resources, particularly for emergency events.

[PR 3] The 6G system shall preserve the semantic information associated with SmartBAN data when it is transferred towards edge- or cloud-based healthcare applications.

[PR 4] The 6G system shall support secure discovery, authentication, authorization, and lifecycle management of Smart Coordinators and associated healthcare services.

[PR 5] The 6G system shall maintain service and application-context continuity when the patient moves between access networks, administrative domains, or edge-service areas.

[PR 6] The 6G system shall support scalable connectivity for multiple Smart Coordinators while preserving isolation among users and healthcare services.

[PR 7] The 6G system shall provide end-to-end protection of sensitive health data between the Smart Coordinator and the authorized healthcare service, including access control and policy enforcement.

3.7. Key Performance Indicators

Relevant KPIs include:

- End-to-end latency from detection of a critical event to its delivery to the healthcare service;
- Reliability of critical-event delivery;

- Service availability;
- Service interruption time during mobility or edge-service relocation;
- Number of simultaneously supported Smart Coordinators;
- Time required for Smart Coordinator and healthcare-service discovery and authorization;
- Communication and processing overhead introduced by the interworking functions.

Numerical targets should be determined according to the clinical criticality of the monitored parameters and the considered deployment scenario.

4.4 Medical Robotic Applications

4.4.1 Adaptive Reconfigurable Exoskeleton-based Home Rehabilitation for Stroke Survivors

1. Description

Stroke is a leading cause of long-term disability, affecting approximately 100,000 people annually in the UK, with over 1.3 million stroke survivors currently living with its effects. Clinical guidelines recommend 45 minutes of rehabilitation therapy, five times per week, yet in practice many patients receive only 1–2 supervised sessions weekly, resulting in recovery rates that can be 2–5× slower. This contributes to a societal cost exceeding £25 billion per year, with long-term care costs of approximately £145,000 per patient over five years. Insufficient rehabilitation intensity and lack of continuous monitoring are key drivers of these outcomes.

This use case describes a home- and community-based rehabilitation system using reconfigurable robotic exoskeletons equipped with integrated biometric and motion sensing. These devices support intensive, personalized rehabilitation in residential settings, enabling patients to perform therapy independently while maintaining clinical oversight.

The exoskeleton continuously captures biomechanical and physiological data (e.g., joint movement, muscle activity, fatigue indicators), which are analysed using personalized AI models to assess recovery status and dynamically adapt therapy routines (e.g., resistance levels, exercise types, repetition rates). Due to the computational complexity of real-time adaptive control and personalization, these AI tasks may be offloaded to the 6G system's Service Hosting Environment, enabling low-latency feedback and scalable processing.

The system operates in a human-in-the-loop rehabilitation pathway, where clinicians remotely monitor patient progress, validate AI-driven adaptations, and adjust therapy plans as needed. This use case bridges the gap between advanced rehabilitation technology (e.g., EPSRC-funded robotic systems) and real-world clinical deployment, enabling scalable NHS adoption.

2. Pre-conditions

- The patient is provided with a reconfigurable rehabilitation exoskeleton (UE) capable of delivering assistive/resistive therapy.
- The exoskeleton includes integrated sensors for motion capture and biometric monitoring (e.g., joint kinematics, muscle activity, heart rate, fatigue indicators).
- The UE supports secure communication with the 6G network.
- A personalized rehabilitation model is initialized using patient-specific clinical data and therapy goals.
- The patient has provided informed consent for continuous monitoring and data processing.

- The 6G system provides access to distributed Service Hosting Environments for AI computation.
- Clinicians (e.g., NHS rehabilitation teams) have access to remote monitoring platforms connected to the system.

3. Service Flows

1. A stroke survivor initiates a rehabilitation session at home using the reconfigurable exoskeleton.
2. The exoskeleton guides the patient through prescribed exercises while continuously collecting motion and biometric data.
3. The UE evaluates local performance metrics (e.g., movement quality, range of motion, fatigue) and detects deviations from expected recovery patterns.
4. The UE generates a compute task to analyse patient performance and optimize therapy parameters using a personalized AI model.
5. Due to computational demands and real-time requirements, the UE requests execution of the compute task in the 6G Service Hosting Environment.
6. The UE transmits relevant data (in a privacy-preserving manner), model context, and execution requirements (e.g., latency, reliability).
7. The 6G system allocates compute and network resources and executes the adaptive rehabilitation model.
8. The model outputs updated therapy parameters (e.g., adjust resistance, modify exercise difficulty, recommend rest periods).
9. The results are returned to the UE, which reconfigures the exoskeleton in real time and provides feedback to the patient.
10. Session summaries and recovery metrics are transmitted to clinicians for remote monitoring and review.
11. Clinicians assess progress and, if necessary, update therapy plans, which are propagated back to the system.

4. Post-conditions

- The patient receives adaptive, high-intensity rehabilitation tailored to their recovery state.
- The exoskeleton dynamically adjusts therapy parameters to optimize recovery outcomes.
- Clinicians maintain continuous visibility of patient progress and can intervene remotely.
- Rehabilitation intensity and adherence increase, reducing long-term disability and care costs.

5. Existing features/requirements partly or fully covering the use case functionality

- Edge computing and distributed service hosting in 5G/5G-A systems enabling compute offloading.
- QoS and network slicing mechanisms supporting latency-sensitive applications.
- Network exposure capabilities allowing applications to request network resources.

However, current systems do not fully support:

- real-time closed-loop control of robotic rehabilitation devices,
- continuous high-frequency sensor data processing,
- integration of personalized AI with clinical workflows,
- strict reliability and latency guarantees required for physical human-machine interaction.

6. Potential new requirements needed to support the use-case

[PR 1] Subject to user consent, the 6G system shall support real-time execution of adaptive rehabilitation compute tasks for robotic exoskeletons in Service Hosting Environments.

[PR 2] The 6G system shall support ultra-low-latency and deterministic communication for closed-loop control of assistive robotic devices.

[PR 3] The 6G system shall support UE specification of task requirements, including latency, reliability, and synchronization constraints.

[PR 4] The 6G system shall support secure, privacy-preserving handling of continuous biometric and motion data streams.

[PR 5] The 6G system shall support lifecycle management and synchronization of personalized rehabilitation AI models across UE and network.

[PR 6] The 6G system shall support integration of clinician oversight, enabling remote monitoring and control.

Operational requirements

[PR 7] The system shall ensure high reliability and safety for human-in-the-loop robotic operation.

[PR 8] The system shall support seamless service continuity across home and community environments.

[PR 9] The system shall provide fallback mechanisms (e.g., safe local control modes) in case of network degradation.

[PR 10] The system shall comply with healthcare regulations and safety standards for medical devices.

7. Key Performance Indicators

- End-to-end control latency: ≤10–20 ms for safe and responsive exoskeleton adaptation.
- Reliability: ≥99.9999% for critical control and feedback loops.
- Jitter: Minimal variation in latency to ensure stable robotic control.
- Task execution success rate: ≥99% for AI-based adaptation tasks.
- Data security and privacy: Full compliance with healthcare data protection standards.

- AI adaptation accuracy: Clinically validated improvement in therapy effectiveness.
- Rehabilitation intensity: Ability to sustain guideline-level therapy (≥45 min, 5×/week).
- Energy efficiency: Support for extended daily use in residential settings.
- Mobility robustness: Seamless operation across different network conditions (home/community).

4.4.2 Tele-surgery

1. Description

Tele-surgery enables a specialist surgeon at a remote site to directly control a robot-assisted intervention on a patient at another clinical site. It can extend access to scarce expertise, reduce treatment delay when patient transfer is impractical, and support planned or time-critical procedures across regional, national and international healthcare networks. A representative high-value scenario is remote robotic endovascular intervention, in which a specialist navigates catheters, guidewires or thrombectomy devices using live fluoroscopic imaging.

The remote surgeon operates a leader console and the patient-side robot executes movements. The surgeon receives clinical video streams, audio, device-state feedback, physiological data and, where supported, haptic feedback. This human-in-the-loop cyber-physical control system has modality-specific communications requirements. Command and state messages are reliability-critical, whereas video requires sustained throughput, low camera-to-display delay, and protection against clinically misleading freezes or corruption. Haptic feedback requires high update rates and bounded jitter, and all modalities require traceable time alignment.

The 6G system provides the communications and distributed-computing environment for the closed control loop. Service hosting at a trusted hospital edge or network edge may support encoding, sensor fusion, visualization and clinically authorized AI.

This is a safety-critical use case. Remote control is enabled only after clinical authorization, device calibration and end-to-end readiness checks. During the procedure, application and network performance are continuously supervised. Figure 1 shows a representative patient-side and operator-side configuration for remote robotic endovascular intervention and the bidirectional communication link between the two sites.

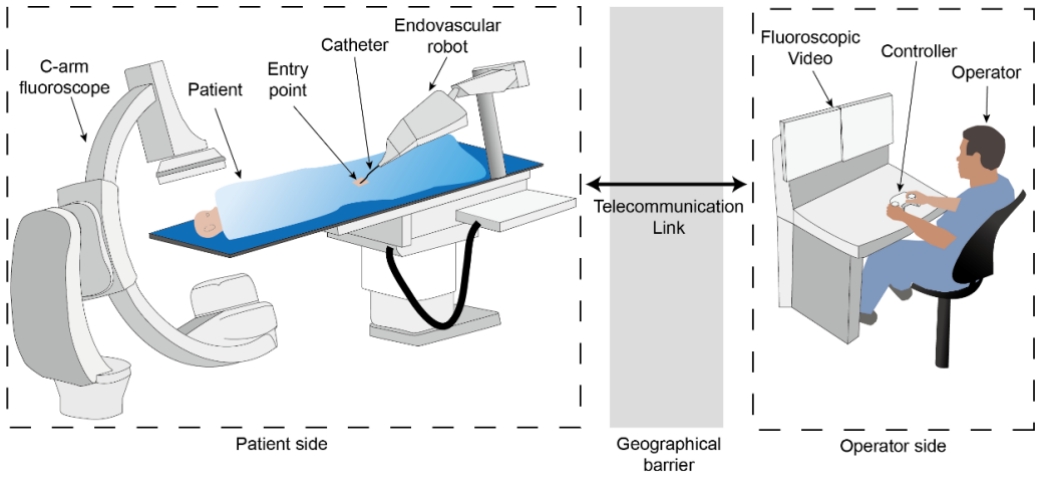

Figure 3 Representative system configuration for remote robotic endovascular intervention.[68] At the patient site, a robotic system manipulates the catheter through the vascular entry point under C-arm fluoroscopic imaging. The remote surgeon operates a leader console and receives live fluoroscopic video from the procedure. The bidirectional telecommunication link carries control commands and procedural feedback across the geographical separation between the two sites.

2. Pre-conditions

- The patient has an appropriate clinical indication for robot-assisted tele-surgery and has provided informed consent for the intervention and the processing of medical, audiovisual and device data.
- The remote surgeon is credentialed to perform the procedure using the robotic platform. A trained patient-side clinical team is present with authority to pause the procedure or assume local control.
- The leader console, patient-side robot, imaging systems, haptic interfaces, patient monitors, gateways and safety controllers are approved for the intended clinical use, mutually compatible and within their validated maintenance periods.
- Both clinical sites have secure, 6G-capable connectivity, trusted gateways and synchronized time sources, with compatible interfaces for command, feedback, video, audio and physiological data streams.
- The remote surgeon and patient-side clinical team have completed simulation-based training for communication loss, hardware or software failure, device malfunction, protective stopping, and emergency conversion to local control.
- A procedure-specific service profile defines the required latency, jitter, reliability, throughput, synchronization, video-quality and edge-computing constraints, together with warning, adaptation and stop thresholds.
- All users, devices and applications are authenticated and authorized; encryption, integrity protection, consent enforcement, data minimization and audit logging are enabled end to end.
- A pre-operative test verifies robotic motion limits, command-to-motion response, camera-to-display delay, audiovisual quality, jitter, packet-loss tolerance, failover behaviour and local emergency controls before the remote control is enabled.

3. Service Flows

Figure 2 summarizes the safety-led service flow, from clinical authorization and service admission to continuous supervision, validated degradation response and local control handover.

1. The clinical teams select the patient and procedure, confirm consent and responsibilities, and securely exchange the relevant surgical plan, imaging and patient information.
2. The remote surgeon, patient-side team, robotic devices and supporting applications authenticate to the service; the system verifies credentials, device status, software compatibility and authorization scopes.
3. The surgical application requests a procedure-specific communication and compute service, including latency, reliability, jitter, synchronization and edge-processing constraints.
4. The 6G system performs admission control, reserves end-to-end resources, establishes primary and backup paths and reports whether the requested communication level can be met.
5. Both teams run the pre-operative connectivity and robotic safety test. The patient-side team prepares the patient, checks instruments and confirms that local emergency controls and local control are available.

6. After safety confirmation, the patient-side controller enables the remote surgeon to take control of the robot within the authorized procedure and motion.
7. During surgery, the leader console sends commands to the patient-side robot while video, audio, device telemetry, sensor data and selected physiological data are returned to the remote surgeon as synchronized streams.
8. The network and application continuously prioritize safety-critical flows, monitor latency, jitter, packet loss, and edge-processing delay, and securely expose performance telemetry to the authorized surgical safety controller.
9. When degradation is predicted or detected, the system adds resources or switches to a validated diverse path without disrupting the control-session state.
10. The remote surgeon performs the planned intervention. The local team supports the procedure, monitors the patient and operating field, and can immediately command a protective stop or assume local control.
11. If any clinical, robotic or security threshold is exceeded, the robot executes the predefined safe response, such as holding position, withdrawing to a safe pose, pausing energy delivery or handing control to the local team.
12. At completion, the remote surgeon returns control to the patient-side team, the robot is placed in a safe state, and the local clinical team completes the procedure and post-operative care.
13. The system securely stores the clinical record together with command and device logs, network-performance, alarms and handover logs for audit, incident review and service improvement.

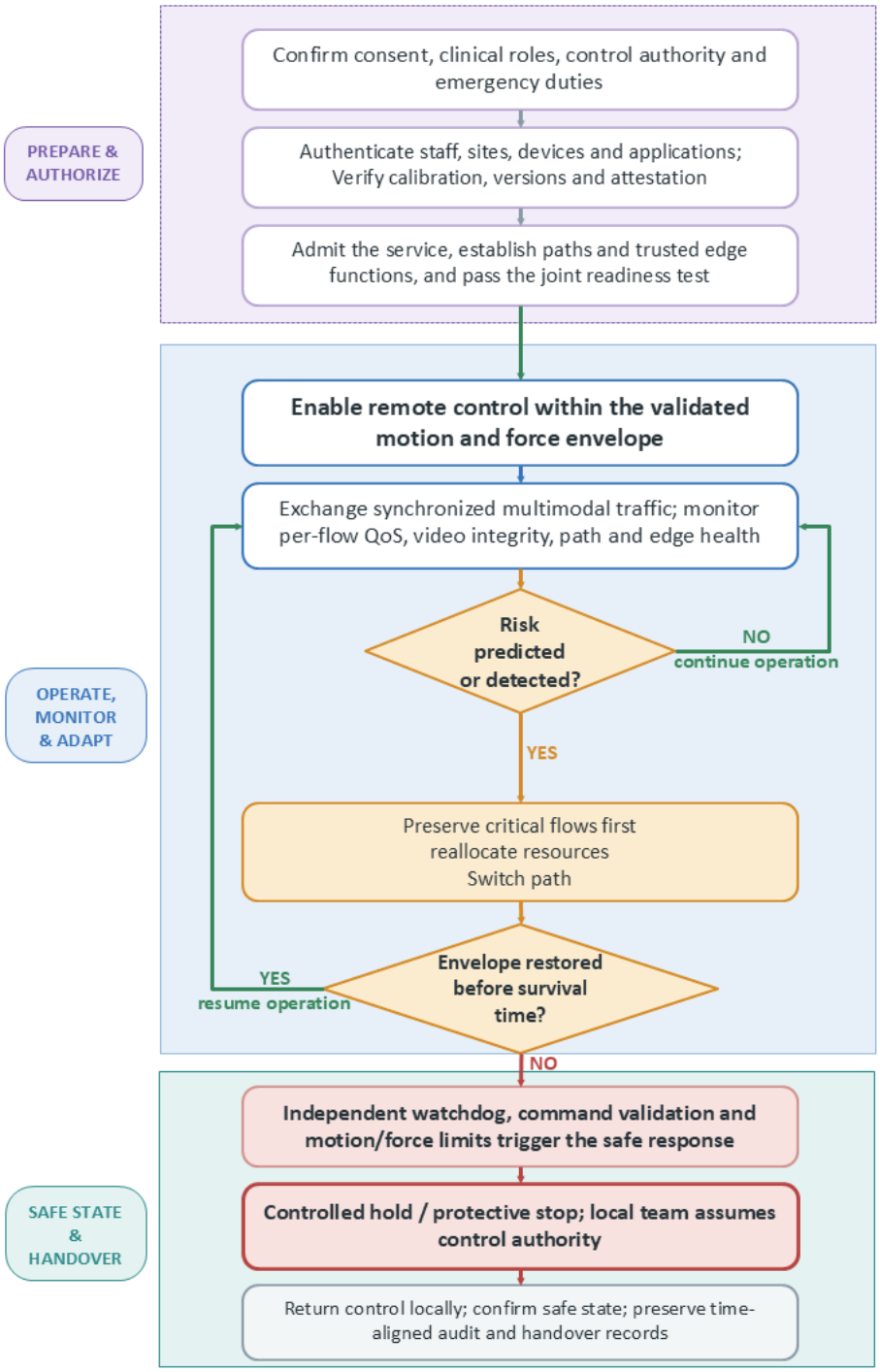

Figure 4 Safety-led service flow and degradation-response logic for tele-surgery. Remote operation is enabled only after consent, control authority, participant authentication, device readiness and the requested communication service have been verified. During the procedure, synchronized multimodal traffic and per-flow performance are continuously supervised. Predicted or detected risk triggers resource reallocation or switching to a validated path while safety-critical traffic retains priority. If the operating envelope cannot be restored before the application survival time, independent patient-side safety functions initiate a controlled hold or protective stop. Control then transfers unambiguously to the local clinical team. Completion requires confirmation of the local safe state and retention of time-aligned audit and handover records.

4. Post-conditions

- The patient remains under the care of the patient-side clinical team, with post-operative monitoring and follow-up arrangements recorded.
- Clinical, robotic, security and network records are time-aligned, integrity-protected and available to authorized parties for the health record, audit and incident investigation.
- Any safety event or performance excursion is reviewed before the service, device configuration or route is approved for a subsequent tele-surgery session.

5. Existing features partly or fully covering the use case functionality

- 5G systems provide enhanced mobile broadband and low-latency communication capabilities that can support clinical video and robotic control.
- Edge computing and local breakout can place video encoding, visualization, sensor fusion and application functions closer to the clinical sites and reduce transport delay.
- Existing security capabilities support subscriber and device authentication, authorization, confidentiality and integrity protection.

6. Potential new requirements needed to support the use case

[PR 1] Subject to clinical and regulatory authorization, the 6G system shall support an end-to-end, bidirectional communications service with bounded latency, jitter, and loss for remote surgical control.

[PR 2] The 6G system shall support synchronized modality-specific transport and priority treatment for command, audio, video, or other clinical video streaming and physiological data.

[PR 3] The 6G system shall expose trusted real-time and predictive performance information, including threshold-crossing and degradation notifications.

[PR 4] The 6G system shall support mutual authentication and fine-grained authorization of clinical staff, sites, devices and applications.

[PR 5] The 6G system shall support standardized safe-degradation, protective-stop and emergency-handover signalling so that the patient-side robot can enter a validated local safe state and transfer control without ambiguity.

7. Key Performance Indicators

The following values are candidate technical targets based on currently available evidence. They should may be updated if stronger or more recent clinical or technical evidence becomes available. Final acceptance limits shall be established through procedure-specific clinical validation and risk assessment, accounting for the specific robotic platform, network architecture, procedure, clinical risk assessment and regulatory context.

- Command and feedback latency: target network contribution of ≤ 50 ms one way, under the nominal service profile, with command-to-actuation delay measured end to end and reported at the 95th and 99th percentiles.

- Camera-to-display delay: target ≤ 150 ms for interactive clinical video, including capture, encoding, transport, decoding and display; a different procedure-specific bound may be justified through clinical validation.
- Critical-flow reliability: packet loss rate ≤ 0.01% within the procedure-specific latency bound, a different robot-specific bound may be justified through clinical validation.
- Jitter: bounded variation for command and feedback flows; a candidate target is ≤ 10 ms at the 99th percentile, subject to the robot and procedure-specific stability analysis.
- Clinical video capacity: Sustained throughput sufficient for the validated visual profile. A candidate is 25 Mbit/s per compressed 1080p30 stream and ≥ 100 Mbit/s aggregate for multiple views or higher-resolution imaging, with uplink and downlink provisioned according to the clinical configuration.
- Multi-modal synchronization: control, haptic, video, audio and patient data remain within procedure-specific alignment limits.
- Performance monitoring: latency, jitter, loss, throughput, synchronization, video-freeze and edge-processing metrics updated at ≤ 50 ms intervals or supplemented by immediate event-driven threshold notifications.
- Video integrity and task visibility: no perceived corruption, freeze or compression artifacts that obscures target anatomy, the operative device or the clinically defined ROI beyond validated limits. PSNR, SSIM and VMAF may be used as engineering indicators.
- Safety response: 100% successful transition to the validated local safe state within the robot-specific stopping time during pre-session and fault-injection tests.

4.5 Immersive treatment

4.5.1 AR/VR enabled patient education

1. Description

The goal of this use case is to use emerging innovative solutions based on augmented reality (AR)/ virtual reality (VR) to the improve knowledge of health conditions, medical procedures, and treatment plans among patients. Instead of relying on 3D static models, 2D scans, or verbal explanations, the patients can now be better informed about their health conditions. Additionally, in case of an upcoming medical procedure, the patient's treatment plan can be visualized and discussed with other care takers to prepare a personalized recovery plan. This is beneficial to reduce patient anxiety and offer necessary health-related measures to improve their well-being and faster recovery.

However, there are several technical challenges associated with such patient education methods. In order for it to be effective, precise virtual modelling of body organs or parts is of utmost importance. To avoid distress to the patients or care-takers, the live consultations with virtual model need to be seamless despite the different AR/VR capabilities among the different participants. Given that health data is confidential, ensuring data privacy and confidentiality in virtual environments with several onsite and remote participants needs to be enabled.

2. Pre-conditions

- The patient's medical information is processed and converted into 3D models for use in the virtual platform by a trusted 3rd party service provider.
- The 6G network offers high-bandwidth, low-latency network, with dedicated QoS to support simultaneous AR/VR and non-AR/VR devices.
- The virtual platform supports asymmetric rendering, enabling seamless visualization on both headsets and 2D screens (tablets/laptops/phones)
- All participants (doctor, patient, remote caretakers) have authenticated and been explicitly authorized to join the session.

3. Service Flows

An example service flow is described below:

1. Bob is diagnosed with a respiratory condition which needs to be treated with a surgical procedure.

2. Bob has arrived at the medical facility to review his condition with the doctor. They use AR/VR headsets to visualize the condition and the treatment procedure.
3. The doctor invites the Bob's caretakers to the virtual platform. The caretakers join either through phones/tablets.
4. The doctor shows the 3D holographic model of the patients' lungs and simulates the treatment procedure in the virtual interactive environment.
5. The patient interacts with the doctor in the virtual platform by making some annotations on the projected 3D picture.
6. The caretakes also interact with doctor and Bob via annotations from laptop, audio.

4. Post-conditions

- The patient and caretakers acknowledge the understanding of the medical condition and treatment procedure.
- The interaction is seamless across multiple participants from different locations and different devices to join the meeting.

5. Existing features/requirements partly or fully covering the use case functionality

3GPP has extensively covered AR/VR features over several releases. These include application-aware QoS handling, distributed processing of XR content between a user device and the network, and categorization of AR-capable devices. Some of the AR/VR requirements relevant to the use case captured in 6G include:

- Subject to operator's policy, the 6G system shall support mechanisms to adapt QoS of the media traffic in an interactive XR communication (e.g. holographic) to achieve consistent user experience under varying network conditions.
- Subject to operator's policy and subscriber permission, the 6G system shall provide a means to synchronise, heterogeneous data flows (including media flows) from/to one or more UEs associated with a single user, and also among UEs associated with multiple users in a multimodal communication.
- Subject to the operator's policy and regulatory requirements, the 6G network shall be able to receive AI-related service requirements from a user /authorised 3rd party as part of a request for an AI service, for example related to AI inference accuracy and latency.
- Subject to operator policy, the 6G network shall be able to support a mechanism to guarantee the user experience when providing combined 3GPP service (e.g. combines 6G AI Service and communication service).

6. Potential new requirements needed to support the use-case

[PR 1] The 6G network shall provide mechanisms to ensure the confidentiality of 3D health-related models and associated data originated from or owned by third-party service providers during storage, processing, and transmission within the network domain.

[PR 2] The 6G network shall support asymmetric rendering, enabling the simultaneous delivery of appropriate media representations to both AR/VR-capable devices and non-AR/VR legacy devices (e.g., 2D smartphones, tablets, or fixed displays) within the same session or service context.

[PR 3] The 6G network shall support real-time sharing of annotations (e.g., spatial markers, labels, or pointers) between AR/VR devices and non-AR/VR devices. This shall be enabled by in-network AI/ML and compute capabilities to perform appropriate translation (e.g., 3D-to-2D projection, coordinate mapping, or semantic abstraction) to ensure consistent interpretation across heterogeneous device types.

4.5.2 AR/VR-Assisted Remote Surgery over 6G Network

1. Description

Surgical procedures increasingly benefit from immersive technologies. Augmented Reality (AR) can overlay real-time patient data, 3D anatomical reconstructions, and navigation guidance directly onto the surgeon's field of view, while Virtual Reality (VR) enables remote surgeons to tele-operate robotic surgical instruments with full immersive visual and haptic feedback. This is particularly valuable in scenarios where specialist expertise is not locally available, e.g. in rural hospitals, disaster areas, or during time-critical interventions where patient transfer is not feasible.

In this use case, a remote specialist surgeon performs (or assists in) a surgical procedure on a patient located in a distant operating room. The remote surgeon wears a VR headset and uses haptic controllers to operate a surgical robot at the patient's site, while the local surgical team uses AR headsets that display the remote surgeon's annotations, vital signs, and AI-generated guidance overlaid on the patient's anatomy. The extremely low latency, high data rate, high reliability, and integrated compute capabilities of the 6G system are essential to ensure that visual, haptic, and control data streams remain synchronized and that the surgeon's actions are executed safely and in real time.

2. Pre-conditions

The operating room is equipped with a surgical robot, high-resolution 3D cameras, and medical sensors (e.g. vital sign monitors, endoscopic imaging), all acting as UEs capable of communicating with the 6G network. The remote surgeon possesses a VR headset and haptic control devices (UEs) connected to the 6G network. The local surgical team possesses AR headsets (UEs) connected to the 6G network. The 6G network provides a Service Hosting Environment capable of executing compute-intensive tasks such as real-time 3D scene rendering, video processing, and AI-based image analysis. Both hospital sites have subscribed to a 6G service with guaranteed quality of service (QoS) for critical medical applications, and all regulatory and patient consent requirements for remote surgery and medical data transfer are fulfilled.

3. Service Flows

1. The local surgical team prepares the patient and activates the remote surgery session. The 6G network establishes end-to-end connectivity between the operating room and the remote surgeon with guaranteed QoS (ultra-low latency, high reliability).
2. The 3D cameras and endoscopic imaging devices in the operating room capture high-resolution volumetric video of the surgical field and stream it via the 6G network.
3. Since rendering photorealistic volumetric video for VR is too compute-intensive for the UEs, a compute task is created and executed in the Service Hosting Environment of the 6G

network, which renders the immersive 3D scene close to the network edge to minimize latency.

4. The remote surgeon views the rendered 3D scene through the VR headset and manipulates the haptic controllers. The control commands are transmitted through the 6G network to the surgical robot with ultra-low latency.
5. The surgical robot executes the surgeon's movements and returns haptic feedback (e.g. tissue resistance, force feedback) through the 6G network to the surgeon's controllers, closing the control loop in real time.
6. In parallel, an AI model executed in the Service Hosting Environment analyses the live video and patient vital signs, detects critical structures (e.g. blood vessels, nerves) and potential anomalies, and generates warnings or guidance.
7. The AR headsets of the local surgical team display the AI-generated guidance, the remote surgeon's annotations, and real-time patient data overlaid on the patient's anatomy, ensuring a shared and synchronized view between the local and remote teams.
8. The 6G network continuously monitors the QoS of all streams (video, haptic, control) and dynamically reallocates communication and compute resources to maintain the required performance. In case of degradation, the network proactively notifies the UEs so that safety procedures (e.g. handover to the local team, pausing robot movements) can be triggered.
9. Upon completion of the procedure, the remote surgery session is terminated and all session data is securely stored for medical documentation purposes.

4. Post-conditions

The surgical procedure is successfully completed with the remote specialist's expertise, despite the geographical distance. The patient receives timely, high-quality surgical care, and a complete record of the session (video, commands, sensor data) is securely archived in compliance with medical data regulations.

5. Existing features partly or fully covering the use case functionality

The 5G system supports Ultra-Reliable Low-Latency Communication (URLLC) with latencies down to 1 ms and reliability of 99.999%, which partially addresses the control loop requirements. 5G also supports network slicing, edge computing (e.g. via ETSI MEC and 5G edge enablers), and QoS differentiation, which partially cover the guaranteed service and edge rendering aspects. However, the 5G system cannot simultaneously guarantee the combination of multi-Gbit/s volumetric video streaming, sub-millisecond haptic feedback latency, deterministic end-to-end synchronization of multiple heterogeneous streams, and integrated network compute offloading with strict execution deadlines required by this use case.

6. Potential New Requirements needed to support the use case

[PR 1] The 6G system shall support mechanisms to execute compute tasks (e.g. volumetric rendering, AI-based image analysis) in the Service Hosting Environment upon service request from UEs, with guaranteed execution deadlines suitable for safety-critical medical applications.

[PR 2] The 6G system shall support mechanisms to jointly allocate and manage communication and compute resources to satisfy the end-to-end latency requirements of a compute task, including transmission, execution, and result delivery.

[PR 3] The 6G system shall support mechanisms to synchronize multiple related data streams (e.g. video, audio, haptic, and control streams) belonging to the same application session, ensuring bounded inter-stream skew.

[PR 4] The 6G system shall support mechanisms to provide deterministic, ultra-reliable, low-latency communication for haptic and robot control traffic simultaneously with high data rate immersive video streams within the same session.

[PR 5] The 6G system shall support mechanisms to monitor the achieved QoS in real time and to proactively notify authorized UEs and applications of predicted or actual QoS degradation, so that application-level safety procedures can be triggered.

[PR 6] The 6G system shall support mechanisms to prioritize and protect resources for critical medical services, including service continuity and seamless failover (e.g. path or edge node switching) without violating the application's latency and reliability requirements.

[PR 7] Subject to regulatory requirements and user (patient) consent, the 6G system shall support mechanisms to ensure end-to-end security, integrity, and confidentiality of medical data, including data processed in the Service Hosting Environment.

7. Key Performance Indicators

To enable the user story defined for this use case, the following KPIs need to be satisfied. The end-to-end latency for the haptic feedback and robot control loop should be at most 1 ms (motion-to-feedback round trip in the order of a few ms), with a communication service reliability of 99.99999% for control and haptic traffic. The volumetric/holographic video streams require data rates in the range of 1–10 Gbit/s per stream in the uplink from the operating room, with a motion-to-photon latency below 10 ms for the VR rendering path to avoid cyber-sickness and ensure surgical precision. Jitter for haptic streams should remain below 0.1 ms, and the synchronization skew between video, haptic, and control streams should not exceed a few milliseconds. The compute task execution in the Service Hosting Environment (rendering, AI inference) must complete within deterministic deadlines in the order of 5–10 ms per frame. Service availability for the overall session should be at least 99.999%, with failover times short enough that no perceivable interruption of the control loop occurs.

4.6 Network-powered healthcare applications

4.6.1 Navigation aid for vision-impaired individuals

1. Description

Navigating through complex outdoor environments could be challenging for individuals with vision impairments. The goal of this use case is to provide navigation assistance primarily via 3GPP sensing and AI/ML capabilities. Upon activation of navigation assistance service by a 3GPP-enabled UE, the mobile network captures the dynamic urban environment via sensing and processes the captured signals to perform key tasks such as scene understanding, obstacle detection, and trajectory planning. Furthermore, the processed information is notified to the individual as audio data to enable real-time navigation guidance.

An overview of the use case is illustrated below.

Figure 5: Illustration of use case on mobile networks based navigation aid for vision-impaired individuals [AI generated image].

2. Pre-conditions

- The 3GPP network is equipped with radio-based sensing capability. The network and the UE are support integrated sensing and communication capabilities.
- The user can register to an assistance service from the network.
- The user can indicate his requirements for the assistance service such as duration of assistance and destination location, among others in different ways, such as text, selection in the assistance mobile application, or a voice command in the mobile application.
- The 3GPP network is capable of processing the command.

- The 3GPP network is capable of processing the sensing signals using trained AI/ML models to perform tasks such as objection detection, environment mapping, and trajectory planning among others.
- The 3GPP network is capable of using trained AI/ML models to transform the processed sensing signals to audio data for the subscriber.

3. Service Flows

An example service flow is described below:

1. Bob, a visually impaired individual, requests navigation guidance via a mobile network operator's mobile application. Bob uses a voice command to make a request, for instance, "Navigate me to the bus stop where bus X is going towards Market Place."
2. The mobile network processes the request and notifies the acknowledgement of the request via audio message.
3. The mobile network configures the sensing and AI/ML processing capabilities as per the request.
4. As Bob starts moving, the mobile network continuously senses the environment and notifies the navigation assistance in a timely manner. The notification is provided as an audio stream to Bob until he reaches his destination.
5. Upon reaching the destination, the mobile network terminates the navigation assistance service.

4. Post-conditions

Bob arrived at the desired destination safely by continuously receiving navigation assistance from the network. The 3GPP network was able to successfully configure the resource (sensing, communication, and AI/ML-related) for the desired duration and operate as per user's requirements.

5. Existing features/requirements partly or fully covering the use case functionality

- Subject to operator's policy, the 6G network shall support mechanisms (e.g., AI capabilities such as AI Agent) to provide suitable 3GPP service or combination of multiple 3GPP services in response to a received request for service (e.g., expressed via Intent(s)) from subscriber/users or an authorized 3rd party.
- Subject to operator's policy, the 6G network shall support mechanisms (e.g., AI capabilities such as AI Agent) to authenticate and authorize a subscriber/user to send an intent to the 6G network.

- The 6G system shall support mechanism to associate the source (e.g., authorized 3rd party, or specific AI Agent) of the intent with subscription information.
- Subject to operator's policy, regulatory requirements and subscriber permission, the 6G system shall support mechanisms (e.g., AI capabilities such as AI Agent) to translate Intent received (e.g., from subscribers/users) into 3GPP services and service performance requirements.
- Subject to operator's policy, the 6G Network shall provide sensing service to detect, classify and count one or more sensing targets

6. Potential new requirements needed to support the use-case

[PR 1] The 6G system shall be able to continuously support sensing service despite sensing target mobility.

[PR 2] The 6G system shall support the translation of network sensing results into multi-modal output, including navigation audio streams, for delivery to an end-user application, while enabling synchronization of the sensing-derived data with the generated audio output.

7. Key Performance Indicators

Apart from the ISAC and AI capabilities related KPIs discussed in 3GPP, some relevant KPIs include:

- Processed sensing result accuracy: For instance, the accuracy of the navigation audio stream generated based on processed sensing results.
- Navigation command related metrics:
    - Navigation command frequency: This metric reflects how frequently the navigation commands are notified to the user.
    - Navigation command freshness: This metric reflects how up-to-date is the navigation command. It indicates whether the command is delivered while still relevant to the current state of the user.

4.6.2 AI-enabled public health alerting

1. Description

Give that the base stations are widely and densely deployed, this use case describes a scenario where 6G networks could offer area-specific public health-related alerts to users. These alerts are generated by collecting data based on user's consent, processing it in an anonymized manner, and generating the relevant alerts. Such services are beneficial during public health emergencies such as outbreaks of infectious diseases during epidemics and pandemics or local environmental hazards (e.g., fires). Local statistics-driven alerts allow individuals to adopt more effective preventive measures. In addition, 6G sensing can support detection of smokey areas due to fire outbreaks, dangerous weather hazards, and allergies in areas.

An overview of the use case is illustrated below.

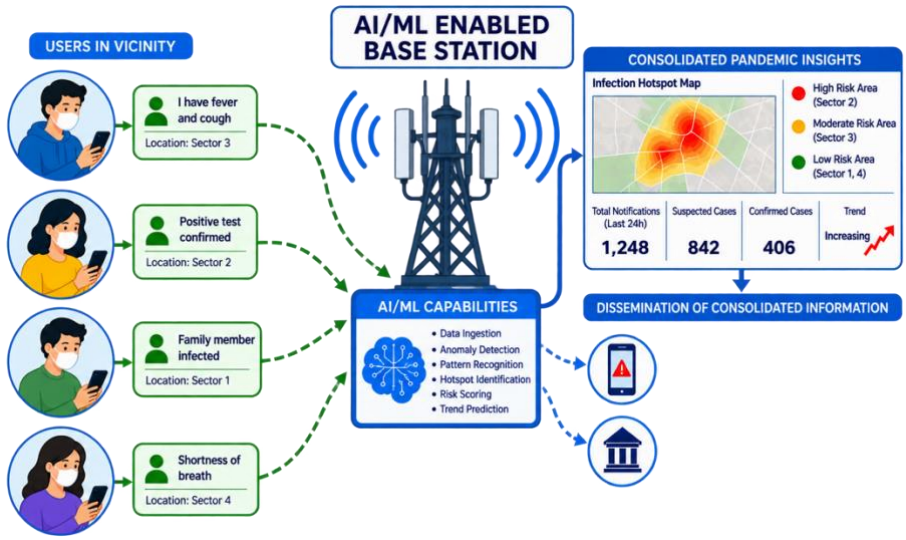

Figure 6: Illustration of AI-enabled public health monitoring use case [AI generated image].

2. Pre-conditions

The mobile network is capable of notifying users in a certain geographical area about the available public health alerts and environmental disruption (which can endanger their health) subscriptions. Users are enabled to subscribe to the alerts directly through the mobile network operators. Mobile network operators are able to collect users' health data and process it in an anonymous and privacy-preserving manner via a user application upon consent. A public health authority has a service agreement with the network operator to request and receive generated alerts from the mobile network operator. The user may decide to update their consent to collect their data at any point in time.

3. Service Flows

An example service flow is described below:

1. A mobile network operator notifies users about available public-health alert subscriptions and data elements collected for each subscription.
2. The users notify the desired data elements when infected or uninfected.
3. Alice relocates to another locality amid the pandemic. She is notified via the mobile network operator application about the available public-health alert subscriptions.
4. Alice subscribes to “Daily alert of total number of infections in Area A” and “Daily new infections forecast in Area A” via the mobile application.
5. Based on the notified data elements and subscribed alerts, mobile network operator processes the data (anonymously and in privacy-preserving manner) to generate the desired daily alerts for Alice. The network leverages the capability of AI/ML models within the network to generate the desired alerts.
6. The public health authority requests generated alerts from the mobile network operator.
7. The mobile network operator provides the requested subscription data to the public health authority for further data aggregation.

4. Post-conditions

The users are notified of the latest public health statistics based on localized information. The public health authority is notified of the desired public-health statistics in a secure way. The AI/ML models are disabled, and data collection and processing is terminated when the public health emergency is officially over.

5. Existing features/requirements partly or fully covering the use case functionality

- Subject to operator’s policy, regulatory requirements and subscriber permission, the 6G system shall provide means for a network operator to monitor network coverage and/or traffic usage, including collection of information form UEs (with subscription to the network operator).
- Subject to operator's policy, regulatory requirements and subscriber permission, the 6G system shall provide mechanisms to efficiently collect, transfer, and process multiple types of data when providing multiple 3GPP services in response to an intent from a subscriber.

6. Potential new requirements needed to support the use-case

[PR1] The 6G network shall be able to dynamically manage user consent and accordingly enable data processing of user data.

[PR2] The 6G network shall enable security and privacy measures appropriate for processing the collected data elements (e.g., location privacy and identity protection).

4.7. Use Case Analysis Conclusions

6G-powered healthcare is not just about faster networks—it is a collaborative multistakeholder endeavour. Based on the use cases presented in [2] and Section 4 of this white paper, the eHealth ecosystem includes doctors, care takers, technology companies, network providers, regulations, and patients themselves. Each group has a vital role to play. At its core, the ecosystem leverages 6G's converged capabilities in communication, sensing, and artificial intelligence to create a shared, data-rich environment.

The white paper's use case clusters and analysis vividly illustrate how these different stakeholders must cooperate across diverse care scenarios. In robotic surgery, for instance, a surgeon in one location, a patient in another, and the robot's manufacturer all depend on each other—and on the network—to ensure that every movement is precise and immediate. Likewise, sensors (wearable or network-based sensing) that monitor patients or users require sensors to be based on algorithm that enable data interpretation in a unified way, and nurses to check the results against the patient's unique condition. When it comes to sharing medical data and AI models, hospitals, researchers, and technology companies must exchange information securely while protecting patient privacy, using common standards so that all systems can "speak the same language." Even immersive treatments, like virtual reality therapy or augmented-reality-assisted procedures, depend on content creators, device makers, and therapists working together to deliver effective care that patients can receive from the comfort of their homes.

The eHealth use cases generate requirements across a wide spectrum, from reliable connectivity and seamless interoperability to stringent safety, security, and privacy protections. They also demand thorough clinical validation to ensure medical efficacy. Clear accountability structure that defines roles and responsibilities across all stakeholders is critical. The following section assess the extent to which the relevant telecommunications, healthcare, medical-device, data and governance standards address these requirements, as well as where gaps or further harmonisation may be needed.

5. 6G-driven eHealth Standards landscape

This section reviews the standards and regulatory landscape relevant to eHealth applications supported by 6G-driven wireless communications. The objective is to identify the principal standards, regulations, and guidance that shape the design, deployment, and operation of healthcare solutions involving sensing, connectivity, data exchange, remote monitoring, and AI-supported interaction.

The standardisation landscape for eHealth is not a single framework that a system either satisfies or fails. It is a composition of safety, cybersecurity, privacy, ethics, and regulatory requirements and is shaped by interactions between these requirements. The problem is that these requirements are each authored by a different community, each has its own vocabulary, and assumptions about who the actors are. Healthcare technology deployments over wireless networks often require a combination of technical standards, legal obligations, and domain-specific guidance that must be mutually comprehensible. However, these requirements are often designed in isolation without considering one another.

This section therefore organises the relevant landscape by **functional categories**, and for each we ask three questions: what does the category actually mean in a 6G driven eHealth context; which instruments (*instrument* is used as a term covering technical standards, binding regulations, and non-binding guidance) govern it; and where current standards provide sufficient coverage, where they are only partially applicable, and where further harmonisation may be needed.

In practice, the implementation of eHealth solutions may involve multiple overlapping instruments, including medical device regulation, AI-related obligations, data governance requirements, and communication standards. The role of standards is therefore not limited to compliance support; they also provide a practical basis for interoperability, assurance, auditability, and risk management across different jurisdictions and deployment contexts.

This section focuses on instruments directly relevant to safety, risk management, cybersecurity, privacy, trust, ethics, interoperability, and compliance in connected healthcare systems. Additionally, the communication infrastructure may also become part of the clinical service chain, which suggests that its standards and regulations should be considered alongside those of the healthcare systems, rather than in isolation. This is particularly important for smart hospitals, remote patient monitoring, robot-assisted rehabilitation, and ambient sensing or AI-driven healthcare support [10].

5.1 Standards categorisation

This section focuses on the standards and regulatory landscape relevant to eHealth applications supported by 6G-driven wireless communications. Healthcare technology deployment over wireless networks often requires a combination of technical standards, legal obligations, and domain-specific guidance that must be mutually comprehensible. The standards landscape is therefore organised into functional layers to show how interoperability, assurance, governance, and values relate to one another across the lifecycle of 6G-driven eHealth systems. The categorisation is not only a structural device; it

also reflects the fact that ethical, legal, and operational concerns in 6G-driven eHealth do not arise in isolation. Different use cases raise different stakeholder concerns, and the ethical analysis must therefore be grounded in the actual system boundaries, the people affected, and the lifecycle stage at which the technology is deployed.

For this whitepaper, the standards landscape is organised into four functional layers: **Values Layer; Assurance Layer; Governance Layer; Network and Interoperability (Infrastructure) Layer**. The rationale for adopting a four-layer structure is that 6G-driven eHealth cannot be understood by listing standards alone and is intentionally ordered to place values and ethical considerations first, followed by assurance, governance, and finally the infrastructure and interoperability foundations that support implementation. A standards catalogue shows what exists, but it does not show how technical interoperability, operational assurance, legal governance, and value-based expectations relate to each other, nor how they map to stakeholder needs. The four-layer approach therefore provides a functional view of the landscape to facilitate connecting use cases to requirements, requirements to standards, and standards to the remaining gaps in harmonisation.

The four-layer structure shown in Figure 7 is ordered to place values and ethical considerations first, followed by assurance, governance, and finally the infrastructure and interoperability foundations that support implementation.

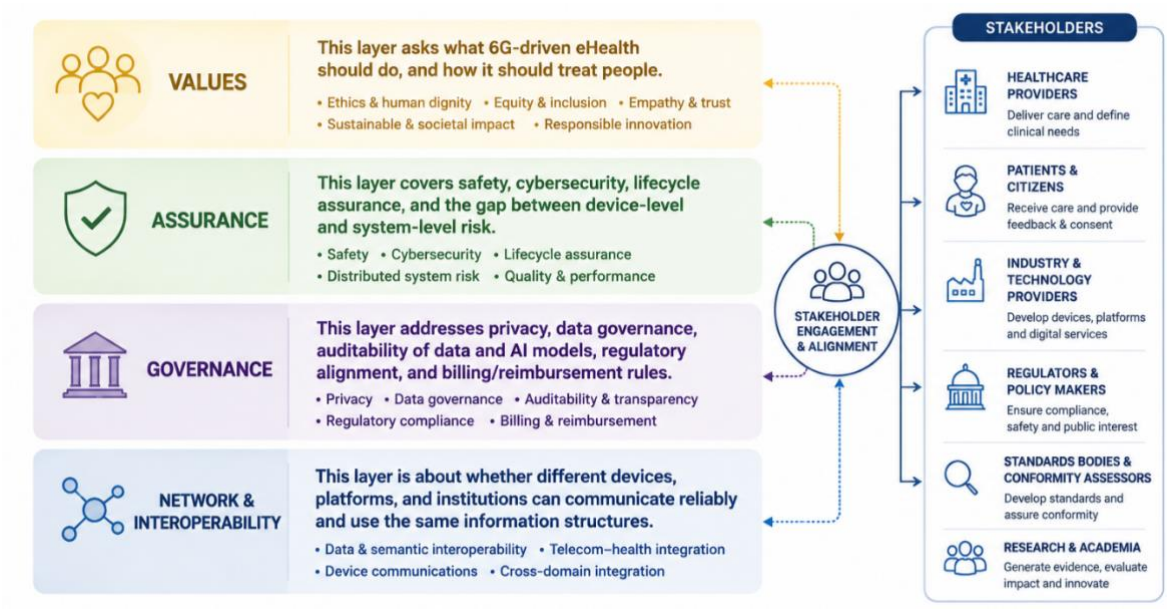

Figure 7: 4-Layer framework for 6G-Driven eHealth

i) Values Layer

At the Values Layer, the paper asks what 6G-driven eHealth should do, and who it serves. The value layer is meant to capture the normative principles that should guide design and deployment rather than the operational controls themselves. The ethics discussion should include all stakeholders affected by a 6G-driven eHealth system, not only healthcare workers and payers, but also patients, loved ones, clinicians, operators, regulators, and others that may be affected depending on the use case. What counts as a stakeholder from an ethical point of view will vary from system to system: most 6G-driven eHealth autonomous or robotic systems will have patients, their loved ones, and medical care workers as stakeholders, but any particular system may add hospital management, network operators, payers, regulators, or service providers. Because the stakeholder set is not fixed, identifying it requires a design activity, which is what the IEEE 7000 series provides a process for.

The IEEE 7000 series Error! Reference source not found. anticipate and incorporate ethical considerations into technology at the earlier (and therefore less expensive and more practical) stages of ideation, specification, and development. Its first standard, **IEEE 7000 Error! Reference source not found.**, provides a general and adaptable process for identifying the ethical stakeholders and potential ethical impacts of a proposed software or AI system, and for developing system specifications that avoid the negative impacts and promote the positive ones.

Other standards in the IEEE 7000 series provide more specific guidance for the kinds of autonomous and robotic systems and systems with intended psychological effects envisaged in this document. **IEEE 7007** Error! Reference source not found. contains definitions, concepts, axioms, and use cases to guide the development of ethical robotic and automated systems. Some of the use cases considered above may influence patient behaviour through subtle means, sometimes called “nudging”. **IEEE P7008** Error! Reference source not found. is a draft standard that describes design, monitoring, and evaluation processes that identify and address ethical considerations posed by AI and autonomous systems that nudge.

The use cases’ autonomous systems must, when they fail, fail in ways that preserve patient safety. **IEEE 7009** Error! Reference source not found. describes methods for creating and using autonomous systems that fail safely. **IEEE P7009.1** Error! Reference source not found. is a draft standard for creating capabilities in autonomous systems that provide for safe interventions in cases of anomalous behaviour. Both are safety-relevant and could be read as Assurance-layer instruments.

Use cases described above must provide communication with a patient or behave near the patient in a manner like that of a caring healthcare worker. That is, in such use cases an AI component of the system emulates empathy. However, emulating empathy poses risks of emotional deceitfulness leading to feelings of abandonment or rejection, risks of emotional over-reliance on an AI system, and other ethical risks. **IEEE 7014** Error! Reference source not found. provides guidance for ethically developing, deploying, and decommissioning autonomous and intelligent systems that, in part, emulate human empathy. The **IEEE 7014.1** standard Error! Reference source not found. adds more specific guidance for emulated empathy when a general-purpose AI system (such as most LLMs) work together with a human.

The robots described in the use cases need to interact with humans: patients and sometimes healthcare workers. **IEEE P7017** Error! Reference source not found. is a standard under development that will provide recommended practices for design, development, and monitoring, of robots providing social assistance to people that provide ethical behaviours and reduce legal conflicts.

At the centre of this analysis is the principle that the patient must never be treated as an object. Ethics is very naturally a value-level concept, and trustworthy AI is often framed as a value-led objective built around fairness, safety, transparency, and human-centred design. Referring to the WHO's ethics guidance for AI in health [30, 31], trust is fundamentally relational; it develops between patients and clinicians, between clinicians and systems, and between the public and institutions. Trust is not an inherent quality of any system; rather, it arises from the relationships involved. Even systems that are technically trustworthy in terms of telecommunications can destroy trusted relationships. In all healthcare, patients must be treated with human dignity, with empathy and due regard for their feelings, and with a clear understanding of what is being done to them and why. In 6G-driven eHealth, this raises the question of how robots and AI systems providing treatment, assistance, emulated empathy, or companionship can support such dignity without misleading the patient. "Mindful dialog" with robots and autonomous systems can help in part, but present LLM-based systems can still drift into deceptive behaviour, including implying feelings or experiences they do not have.

Some flexibility comes from the principle of double effect **Error! Reference source not found.**, which recognises that some harm may be permitted, or even a risk of considerable harm taken, if doing so is unavoidable to save a life or restore someone to optimal living. Triage is a related issue: triage decisions must ultimately be made by someone with clear accepted medical judgment and moral authority, and patients, loved ones, and other stakeholders must be able to believe that the decision-maker is acting in the best possible way under the circumstances. Beyond the question of deciding who can be saved, no AI, robot, or automation may select, nor be perceived as selecting, who is worthy or not.

The societal impact of widespread robotics and autonomy in medical care also needs explicit treatment. Potential concerns include alienation of patients and loved ones, reduced confidence that healthcare providers are listening or empathising, and wider concerns about how

automated care may reshape the patient–provider relationship. Environmental impacts should also be considered, including the resource burden of large-scale AI deployment.

ii) Assurance Layer

At the **Assurance Layer,** the focus is on cybersecurity and lifecycle assurance, together with safety and risk management. This layer covers secure development, identity and access control, resilience, vulnerability handling, patching, and safety validation across the lifecycle of connected healthcare systems. Safety, in this category, is freedom from unacceptable harm to a person, such as physical or physiological damage to the patient or clinician, property, or the environment, and risk is the product of the severity and probability of that harm, as captured in ISO 14971 [27]. Risk management is then the disciplined, documented process by which hazards are identified, their severity and probability estimated, controls applied, and residual risk judged acceptable in light of clinical benefit.

Security, in this same category, is not the confidentiality of a link but the discipline of keeping a health system safe and effective in the presence of an adversary, across its whole life: from threat modelling and secure design, through vulnerability handling and disclosure, to patching a device that is already in use on a patient. What distinguishes health-sector security from information security generally is its failure mode, which is not data loss but patient harm. Cybersecurity and lifecycle assurance are therefore treated in the same layer as safety, because 6G-driven eHealth depends on secure and resilient connectivity, secure software, and lifecycle controls that extend beyond the device boundary.

The main and most recent governing instrument for safety and risk management is ISO 14971:2019 [30], the medical-device risk management standard, which brings data and cybersecurity risks into the clinical risk process rather than treating them as a parallel track.

Additionally, considering the use cases [1], [2] **or** Section 4 of this paper, several use case-specific standards also exist, as cited in Table 1. **IEC 60601** family covers basic safety and performance requirements for medical electrical equipment; **IEC 80601** applies to medical robots for rehabilitation, assessment, compensation, or alleviation; **ISO 13482** covers safety requirements for personal care robots; **ISO 3691-4** covers driverless navigation of robotic fleets in hospital corridors; **IEC 62304** and **IEC 82304-1** address software lifecycle and health software product requirements; and **SOTIF (ISO 21448)** is included here as a borrowed analogy from the automotive domain: it addresses hazards arising from functional insufficiency rather than component failure, which is precisely the failure mode of a sensing or AI-driven clinical function, but no adopted health-sector equivalent yet exists. These standards assume that the safety function resides inside the device, and the gap in safety at the system level is obvious.

IEC 80001-1 [8] is particularly relevant where medical devices are connected to hospital or clinical networks, because it frames risk management at the system level rather than at the device level alone. This is important for smart hospital use cases, remote monitoring, and networked rehabilitation, where communication performance and device behaviour may directly affect clinical outcomes. **IEC 81001-5-1** [9] addresses the security of health software across the lifecycle, which is essential where software updates, remote access, cloud integration, or AI-supported functions are part of the solution. For 6G-driven eHealth, such matters because connectivity, software logic, and cybersecurity become tightly coupled and must be managed together. NIST work on medical device interoperability **Error! Reference source not found.** and securing

connected medical devices reinforces device integrity, data protection, and cyber resilience as design requirements rather than afterthoughts.

IEC 80001-1 nonetheless presumes an accountable healthcare delivery organisation in control of the network to which the devices connect. No standard governs a distributed safety function that crosses out of that organisation's control: for instance, **ISO 13482** has no concept of a safety function whose sensor is owned by a mobile network operator, and IEC 80001-1 offers no mechanism for allocating residual risk across that boundary. The gap in safety at the system level is therefore not closed by extending risk management to the hospital network; instead, the gap re-emerges at the network's edge.

iii)Governance Layer

At the **Governance Layer**, the paper addresses privacy, data governance, auditability, regulatory alignment, and compliance. Privacy, in this layer, is a data governance property rather than a security property: it holds that data should have been collected for a stated purpose, on a lawful basis, with the knowledge of the person it describes, retained no longer than necessary, and accounted for. Confidentiality (i.e. preventing leakage or the revealing of personally identifiable information) is a security control that serves privacy but does not constitute it, since data that should never have been collected is not made private by being well protected. Considering the patient's side, the same property as defined by **NCHICA** (North Carolina Healthcare Information and Communications Alliance), is the right of an individual "to control the acquiring, use or release of his or her personal health information" [46]-[48]. Informed consent should also be explicitly recognised as a core governance and ethics requirement, particularly where medical procedures or the use of personal health data require patient authorisation under applicable legal and regulatory frameworks.

Regulatory philosophy is increasingly shifting from a one-time compliance mindset toward ongoing monitoring, post-deployment oversight, and incident reporting for AI-enabled healthcare systems. The relevant privacy governing instruments include **GDPR**, the **EHDS** regulation, **HIPAA**, and **ISO/IEC 27701:2025**, the Privacy Information Management System standard, which also encompasses biometric data, health data, IoT, and AI-related privacy risks. Auditability is about the data, but it is also about the auditability of the whole AI model, including data as part of its lifecycle. Regulatory alignment and compliance should remain in this layer as well, since medical device regulation, jurisdiction-specific healthcare rules, certification, and conformity assessment schemes shape deployment across different legal environments. In addition to

technical standards, healthcare deployments must also reflect legal and regulatory instruments. In Europe, these include medical device regulation**Error! Reference source not found.**, data protection obligations **Error! Reference source not found.**, and the **AI ActError! Reference source not found.**, while in the **United States HIPAA Error! Reference source not found.**-**Error! Reference source not found.** remains a significant reference point for health data privacy and security. For connected medical devices and associated software, the regulatory picture is therefore not limited to one instrument, but depends on the interaction between healthcare law, AI legislation, data protection, device rules, and technical standards. Billing standards for eHealth services also belong here, because they are part of the operational and regulatory framework for implementation rather than the technical communications stack.

iv)Network and Interoperability Layer

The **Network and Interoperability Layer** is anchored by **ITU-R IMT-2030** (aka 6G), **3GPP Releases 20**, **IEC**, **HL7 FHIR**, **IHE profiles**, and **ISO 13940** (ContSys), which supplies a system of concepts for continuity of care, together with the wider **ISO/TC 215** health informatics portfolio, and it covers the standards and guidance that enable interoperability and communications in 6G-driven eHealth. At the Network and Interoperability Layer, this paper examines how previous and present standardisation efforts support interoperability in 6G-driven eHealth use cases through Health Level 7 (HL7)[51], FHIR R4/R5/R6[50], IHE profiles, DICOM[58], and XDS, in relation to IEEE, IEC [8][67][67], CE markings, NIST **Error! Reference source not found.**-**Error! Reference source not found.**, HIPAA **Error! Reference source not found.**-**Error! Reference source not found.**, GDPR **Error! Reference source not found.**, and WHO **Error! Reference source not found.**,**Error! Reference source not found.**. HL7 v2, introduced in 1987, was built around pipe-and-hat delimited messages such as ADT, ORU, and ORM. It succeeded operationally, but failed semantically, because it moved data reliably but said little about what the data means beyond a shared reading of a specification that must be customized by individual sites. It remains the most widely deployed layer interface standard in legacy hospital environments worldwide, largely because it is loosely specified. In other words, every vendor implements a slightly different flavour, which made local adoption easy but cross-institution interoperability fragile.

FHIR, an HL7 standard and an evolution of HL7, is the current leading approach for healthcare data exchange and represents a significant advance from earlier HL7 messaging frameworks. However, its adoption has not fully resolved interoperability challenges; rather, it has shifted the remaining issues toward semantic alignment, data governance, and consistent implementation. This persistence of technical exchange without semantic closure means that standardisation has advanced unevenly across the stack. The main consequences of HL7's evolution are version fragmentation, proliferation of implementation guides, and an assurance and governance layer that has not kept pace with the network and interpretability layer. With the continued adoption of 6G-driven eHealth, and as healthcare moves from connected to intelligent systems, further use of FHIR R4, the trial-use R5 release, and the emerging R6 release will continue to shape interoperability in 6G-driven eHealth use cases. These releases help address some of the limitations associated with earlier HL7 messaging approaches at both local and global levels of interoperability. Another persistent challenge across HL7's evolution is that governance and assurance have often lagged behind technical standardisation. In FHIR integration, it should be made clear that AI cannot substitute for structural interoperability, as standardised structured

data remains a prerequisite for trustworthy AI in 6G-driven eHealth systems rather than a problem that AI can route around [49][52].

The **IEEE eHealth standards** portfolio provides an important interoperability foundation, particularly for medical device communications, wireless networking, and multi-vendor integration. **NIST**'s medical device communication and interoperability work complements this by emphasising testable assertions, message validation, terminology alignment, and conformance testing. This is especially relevant where the whitepaper considers the interface between telecom systems and healthcare systems, and where standardised communication profiles are needed to support scalable deployment in multi-vendor environments.

It is worthy to fully understand what 6G can do and will do in the context of 6G-driven eHealth, beyond what 5G can already support [31] in secure connectivity and networked healthcare services. While 5G enables reliable communication, network segmentation, and secure non-public health enterprise networks, 6G is expected to go further by supporting AI-native networking where the network itself can contribute to clinical decision-making, digital twins where a virtual copy of each patient can be maintained, semantic communication where meaning rather than raw data is transmitted, integrated sensing and communication (ISAC)[68] where the network can detect vital signs through contactless measurement, intelligent edge processing where diagnosis occurs near the patient, and network intelligence that supports a shift from evidence-based to model-based personalised medicine. This will keep pushing the ethics chapter to evolve from discussing "Responsible AI" to defining "Ethics-by-design" for native AI healthcare networks. 6G-driven eHealth will not simply transport data; it will increasingly participate in healthcare decision-making, which elevates ethics from just compliance to a core system design requirement.

First one6G 6G & eHealth whitepaper [1] stated ethical principles like trustworthy AI, privacy, security, transparency, and sustainability, but has not included measurable implementation guidance. Similar to how telecom standards define metrics for latency, throughput, and reliability, 6G-driven eHealth could expose measurable ethical indicators, including AI explainability score, fairness score, consent compliance score, privacy assurance score, sustainability score, clinical safety score, and human oversight score and could potentially enable all these metrics into the future 6G standards IMT-2030.

Table 1: Standard landscape: Goal, Scope, and Functional Layers

Layer	Purpose and scope	Key stakeholders	Representative standards, regulations, guidance
	Guide ethical design, human oversight, fairness, and trustworthiness.	Patients, clinicians, policymakers, ethics boards, public-interest stakeholders	WHO ethics guidance for AI in health; WHO Global Strategy on Digital Health 2020–2025; UN SDGs; IEEE 7000 series; IEEE 7007; IEEE P7008; IEEE 7009; IEEE P7009.1; IEEE 7014; IEEE 7014.1; IEEE P7017, IEEE 7010

Layer	Purpose and scope	Key stakeholders	Representative standards, regulations, guidance
	Provide safety, cybersecurity, resilience, and lifecycle assurance for connected healthcare systems.	Device vendors, network operators, hospitals, safety engineers, cybersecurity teams	ISO 14971:2019 / Amd 2:2024; IEC 80001-1; IEC 60601 family; IEC 80601; ISO 13482; ISO 3691-4; IEC 62304; IEC 82304-1; SOTIF/ISO 21448 (automotive; borrowed analogy, no health equivalent adopted); IEC 81001-5-1; IEC 62443, ISO/IEC 27001, IEEE 2621.
	Support privacy, auditability, compliance, and regulatory alignment for deployment across jurisdictions.	Regulators, hospital management, legal teams, compliance teams, data controllers	GDPR; EHDS regulation; HIPAA; ISO/IEC 27701:2025; medical device regulation; national healthcare rules; certification and conformity assessment schemes; billing standards for eHealth services, ISO/IEC 27018.
	Enable data exchange, semantic alignment, and service interoperability across 6G-driven eHealth systems.	Network operators, vendors, system integrators, hospitals	ITU-R IMT-2030; 3GPP Releases 20; HL7 v2; HL7 FHIR R4/R5/R6; IHE profiles; DICOM; XDS; ISO 13940; ISO/TC 215; IEEE eHealth standards portfolio; IEEE 11073; ETSI ISAC; NIST medical device communication; NIST medical device interoperability; NIST RTMMS; NIST wireless medical device interoperability, DICOMweb, OMOP CDM.

This categorisation in Table 1, is intended to make the analysis easier to follow and to support later gap analysis, because 6G-driven eHealth deployments usually require a combination of technical standards, legal obligations, and domain-specific guidance rather than a single framework. Complementary short-range wireless technologies specifically designed for body-area and medical-device communications, such as ETSI SmartBAN [60]-[63], IEEE 802.15.6 [64], and IEEE 802.15.4j [66], are relevant to eHealth deployments involving wearable sensing and local medical device connectivity, as adjacent enabling technologies.

The standards landscape should be read in conjunction with the stakeholder-driven use cases. Smart hospitals, remote patient monitoring, robotics-assisted rehabilitation, and ambient sensing all rely on a combination of safety, security, interoperability, and governance requirements. As a result, the standards applicable to each use case may differ in emphasis, but the underlying need for trustworthiness, accountability, and deployment readiness is shared. Particularly, it will assist in the selection of applicable standards to support any legal requirements that might apply.

5.2 Standards gaps and need for harmonisation

The purpose of this section is not to list standards again, but to read the landscape of Section 5.1 against the use cases to show where the standards base is sufficient, where it is only partially applicable, and where further harmonisation or 6G-specific work is still required. The four-layer structure is used as the organising axis, so that each gap can be attributed to a layer and, through Table 1, to the standards communities that would have to close it.

Across the standards landscape, several recurring expectations emerge. These include safe interoperability, reliable connectivity, strong identity and access control, traceability, data governance, privacy protection, and lifecycle security. In eHealth, these are not optional enhancements; they are baseline conditions for trust and deployment readiness.

A key challenge is that these expectations are spread across different standards communities and regulatory domains. A further gap is the need for a lifecycle view of autonomous healthcare systems: design and development, commissioning, monitoring and governance, and decommissioning. Ethical considerations change across these stages, rather than treating ethics as a single design-time concern, so ethics cannot be treated as a single design-time concern. Implementation teams therefore need to interpret multiple instruments together, and not assuming that a single standard or regulation is sufficient on its own.

Although the current standards base provides a solid foundation, several gaps remain when viewed from the perspective of 6G-driven healthcare [2]. These include the need for clearer guidance on communication-layer support for clinical safety, stronger alignment between network assurance and medical-device assurance, and more explicit treatment of ethics, auditability, and trustworthy AI in connected care environments. When assessed across the four layers, these gaps fall as follows. At the Network and Interoperability Layer, the gap exists between a communication service and a clinical record. At the Assurance Layer, the gap is the one identified in Section 6.1: safety functions that leave the device. At the Governance Layer, the gap relates to issues of consent and jurisdiction, and at the Values Layer, the gap is measurability.

There are also gaps in the regulation of health data sharing or international transfer of health data in various parts of the world. In Africa, for example, there is not a standard definition of health data applied in all current data protection laws, and cross-border transfer of data is not regulated adequately. The pattern is more general: most countries have data protection laws, but this does not mean that the same level of protection applies everywhere, and an important open question worldwide is how well international transfer of personal data is legally protected. There is a thus a need for harmonisation of legislation and standardisation of key concepts.

The standards review above provides the basis for a structured cross-domain gap analysis. The purpose of this analysis is to translate stakeholder needs and use-case requirements into a consolidated set of technical, operational, and governance requirements that can guide future standardisation and implementation.

5.3 Consolidated requirements

The consolidated requirements should prioritise the capabilities most critical for clinical usefulness and deployment readiness. In practice, this means identifying requirements such as deterministic connectivity where needed, secure and verifiable device integration, robust identity and access control, privacy-preserving data flows, explainable and auditable AI functions, graceful degradation under faults or disruptions, and lifecycle-aware governance for autonomous and AI-supported healthcare systems.

This section therefore provides a high-level consolidation of the most relevant requirements, while the more detailed mapping from requirement categories to candidate standards, maturity assessment, and priority is reserved for future work. That future work should use the four-layer structure developed in this paper to make explicit where the standards base is mature, where it is only partially applicable, and where additional 6G-specific guidance is still missing.

Further work is required to develop a concise set of harmonised requirements that can support future whitepapers, standards contributions, and implementation guidance. These requirements should also reflect the ethical scope of 6G-driven eHealth, including the need to account for all relevant stakeholders and for the full lifecycle of the system, from design and development through commissioning, monitoring and governance, to decommissioning. Emerging 6G-driven healthcare applications may extend beyond patient monitoring to logistics, including autonomous delivery of emergency medical supplies such as automated external defibrillators (AEDs), blood products, or medicines [53].

A possible way to structure the list is to group requirements so that they reflect both deployment needs and the four-layer structure used in this work, with the detailed traceability and priority assessment reserved for subsequent analysis.

6. Conclusion and Next Steps

This white paper has demonstrated that the future of eHealth is not defined by any single technological breakthrough, but by the successful integration of diverse innovations within a robust, standardised framework. The journey from novel use cases to widespread deployment is paved with the collaborative efforts of different stakeholders.

Based on our analysis, the envisioned 6G is set to support and amplify healthcare advancements. It could be considered as an underlying fabric that has the potential to make new care models possible. In addition to the healthcare use cases being currently discussed in SDOs and previous version of the white paper [1][2], several new use cases (and clusters) and requirements have been identified in this white paper. The new use case clusters include: Agentic AI health monitoring, Cross-Standards integration, and AI-enabled mobile network for healthcare applications. From the analysis of use cases in these categories, the proposed technical enhancements to the upcoming 6G networks include support for agents in the network, enabling interaction between UE agents and network agents, translation of high-level intents into appropriate network configurations, enabling internetworking of multiple eHealth related devices operating with different standards, and mobile networks operating a data handlers of health data by ensuring the necessary data privacy and anonymity requirements. Additionally, the new use cases analysed in the previously identified use case clusters [2] have brought to light some valuable requirements such as privacy-aware outdoor sensing, support for real-time execution of compute tasks in service hosting environments, UE specification of compute task requirements, synchronization of modality-specific transport and priority treatment of different traffic, and synchronized co-existence of AR/VR and non-AR/VR streams, and fallback mechanisms in case of network degradation, to name a few. Although 6G may support capabilities such as sensing, analytics for medical decision support, clinical responsibility and final decisions remain subject to clinical governance and professional accountability. Safe deployment depends on interoperability, lifecycle assurance, governance, ethics, clinical validation and stakeholder coordination.

This evolution in eHealth is being actively guided by several standardization bodies spanning multiple domains as elaborated in the four-layer functional categorization (Values, Assurance, Governance, and Network and Interoperability) discussed in Section 5. When assessed across the four layers, the identified gaps are as follows: At the Network and Interoperability Layer, the gap exists between a communication service and a clinical record. At the Assurance Layer, the gap is safety functions that leave the device. At the Governance Layer, the gap relates to issues of consent and jurisdiction, and at the Values Layer, the gap is measurability.

Based on the eHealth related analysis in one6G so far, the main recommendation and next steps include: a further and deeper analysis of use case requirements beyond traditional connectivity needs encompassing the full spectrum of 6G's transformative capabilities. This means dissecting each use case to uncover new requirement dimensions. This could result in a rich, multi-dimensional requirements framework that can beneficially guide system developers and mobile communication standardization activities. Additionally, refining use case descriptions from a holistic perspective, meaning, examining them across clinical, technical, operational, and regulatory dimensions simultaneously, rather than in isolation. This integrated view uncovers gaps that single-domain analysis might overlook. These identified gaps then serve as targeted inputs for multiple Standards Developing Organizations (SDOs), including 3GPP, HL7, IEEE, and ISO, each of which addresses different layers of the eHealth ecosystem. The proposed four-layer functional categorization of the eHealth standards landscape can be used as a basis to reduce duplication, accelerate consensus, and ensure that the resulting standards are coherent and interoperable across domains—transforming use cases from simple illustrations into practical roadmaps for coordinated standardization.

References

[1] one6G Association, "6G Vertical Use Cases," White Paper, June 2022. Available: https://one6g.org/download/2027/

[2] one6G Association, "6G & eHealth: Use Cases and Potential Service Requirements," White Paper, Sep. 2024. Available: https://one6g.org. Accessed: Jul. 1, 2026.

[3] ETSI. ETSI GR ISC 001 V1.1.1: Integrated Sensing And Communications (ISAC); Use Cases and Deployment Scenarios. European Telecommunications Standards Institute, Mar. 2025.

[4] 3GPP. 3GPP TR 22.870 V20.0.0: Study on 6G Use Cases and Service Requirements; Stage 1 (Release 20). 3rd Generation Partnership Project, Mar. 2026.

[5] https://www.nursingtimes.net/archive/nurses-waste-an-hour-a-shift-finding-equipment-10-02-2009/

[6] https://digital-strategy.ec.europa.eu/en/library/2018-report-implementation-european-emergency-number-112

[7] ETSI, ETSI TR 103 944: Smart Body Area Network (SmartBAN); Technical Report on Smart Coordinator for SmartBAN networks. European Telecommunications Standards Institute, 2023.

[8] IEC, "IEC 80001-1:2021: Application of risk management for IT-networks incorporating medical devices — Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices," ISO. [Online]. Available: https://www.iso.org/standard/44863.html. Accessed: Jul. 1, 2026.

[9] IEC, "IEC 81001-5-1:2021: Health software and health IT systems safety, effectiveness and security — Part 5-1: Security activities in the product life cycle," VDE Verlag. [Online]. Available: https://www.vde-verlag.de/iec-normen/250590/iec-81001-5-1-2021.html . Accessed: Jul. 1, 2026.

[10] IEEE Standards Association, "IEEE eHealth Standards Collection," Sep. 2019, [Online]. Available: https://standards.ieee.org/wp-content/uploads/import/documents/other/ehealth.pdf . Accessed: Jul. 1, 2026.

[11] NIST, "Medical Device Communication." [Online]. Available: https://www.nist.gov/healthcare/medical-device-communication . Accessed: Jul. 1, 2026.

[12] NIST, "Medical Device Interoperability." [Online]. Available: https://www.nist.gov/programs-projects/emerging-technologies-healthcare/medical-device-interoperability . Accessed: Jul. 1, 2026.

[13] NIST, "Medical Device Communication — RTMMS." [Online]. Available: https://www.nist.gov/itl/medical-device-communication-rtmms . Accessed: Jul. 1, 2026.

[14] NIST, "Advancing Wireless Medical Device Interoperability." [Online]. Available: https://www.nist.gov/document/md-whpc-wireless-medical-device-interoperability-overview . Accessed: Jul. 1, 2026.

[15] NIST, "Just Published | Final SP 800-66r2, Implementing the HIPAA Security Rule." [Online]. Available: https://www.nist.gov/news-events/news/2024/02/just-published-final-sp-800-66r2-implementing-hipaa-security-rule . Accessed: Jul. 1, 2026.

[16] NIST, "SP 800-66 Rev. 2, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." Feb 2024 [Online]. Available: https://csrc.nist.gov/pubs/sp/800/66/r2/final . Accessed: Jul. 1, 2026.

[17] U.S. Department of Health and Human Services, "HIPAA Home." [Online]. Available: https://www.hhs.gov/hipaa/index.html . Accessed: Jul. 1, 2026.

[18] U.S. Department of Health and Human Services, "The HIPAA Privacy Rule." [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html . Accessed: Jul. 1, 2026.

[19] U.S. Department of Health and Human Services, "Summary of the HIPAA Privacy Rule." [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html . Accessed: Jul. 1, 2026.

[20] European Commission, "Artificial Intelligence in healthcare." [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en . Accessed: Jul. 1, 2026.

[21] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)." [Online]. Available: https://www.legislation.gov.uk/eur/2016/679/contents . Accessed: Jul. 1, 2026.

[22] European Union, "Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices." [Online]. Available: https://www.medical-device-regulation.eu/download-mdr/ . Accessed: Jul. 1, 2026.

[23] European Union, "Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)." [Online]. Available: https://artificialintelligenceact.eu/the-act/. Accessed: Jul. 1, 2026.

[24] NCBI Bookshelf, "Governing AI in the European Union: emerging infrastructures and regulatory ecosystems in health." [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK613197/?report=reader. Accessed: Jul. 1, 2026.

[25] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing, 1*(1), 11–33.

[26] M. A. Houghtaling, S. R. Fiorini, N. Fabiano, P. J. S. Gonçalves, O. Ulgen, T. Haidegger, J. L. Carbonera, J. I. Olszewska, B. Page, Z. Murahwi, and E. Prestes, "Standardizing an Ontology for Ethically Aligned Robotic and Autonomous Systems", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 54, no. 3, pp. 1791-1804, March 2024.

[27] A. Alves, F. Aldeed, and P. J. S. Gonçalves, "Towards Ethically Driven Social Service Robots for Older Adults Care," in Proc. IEEE Int. Conf. on Autonomous Robot Systems and Competitions (ICARSC), 2026.

[28] IEEE Standards Association, "Autonomous and Intelligent Systems (AIS) Standards - IEEE 7000 Series," IEEE SA, 2022.

[29] IEC, IEC 62443 (all parts), [Online]. Available: https://www.iec.ch/cyber-security. *Accessed: Jul. 16, 2026.*

[30] ISO 14971:2019/Amd 2:2024, "Medical devices — Application of risk management to medical devices."

[31] M. Ghassemian, M. Smith-Creasey, and M. Nekovee, "Secure non-public health enterprise networks," in Proc. IEEE Int. Conf. on Communications Workshops (ICC), 2020

[32] *World Health Organization, Ethics and governance of artificial intelligence for health, Geneva: WHO, 2021.*

[33] *World Health Organization, "Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models," Geneva: WHO, 2024 (rev. 2026). [Online]. Available:* https://www.who.int/publications/i/item/9789240084759. *Accessed: Jul. 16, 2026.*

[34] A. G. Nienaber McKay, D. Brand, M. Botes, N. Cengiz, and M. Swart, "The regulation of health data sharing in Africa: a comparative study," J. Law Biosci., vol. 11, no. 1, lsad035, Jan. 2024. [Online]. Available: https://doi.org/10.1093/jlb/lsad035. Accessed: Jul. 16, 2026.

[35] A. McIntyre, "Doctrine of Double Effect," The Stanford Encyclopedia of Philosophy, Winter 2023 ed. [Online]. Available: https://plato.stanford.edu/archives/win2023/entries/double-effect/. Accessed: Jul. 10, 2026.

[36] IEEE Standards Association, Autonomous and Intelligent Systems (AIS) Standards, [Online:] Available: https://standards.ieee.org/initiatives/autonomous-intelligence-systems/standards/, Accessed 10 July 2026.

[37] IEEE, IEEE 7000-2021: IEEE Standard Model Process for Addressing Ethical Concerns during System Design, [Online:] Available: https://standards.ieee.org/ieee/7000/6781/, Accessed 10 July 2026.

[38] IEEE, IEEE 7007-2021: Ontological Standard for Ethically Driven Robotics and Automation Systems, [Online:] Available: https://standards.ieee.org/ieee/7007/7070/ Accessed 10 July 2026.

[39] IEEE, IEEE P7008: IEEE Draft Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems, [Online:] Available: https://standards.ieee.org/ieee/7008/7095/ Accessed 10 July 2026.

[40] IEEE, IEEE 7009-2024: IEEE Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems, [Online:] Available: https://standards.ieee.org/ieee/7009/7096/ Accessed 10 July 2026.

[41] IEEE, IEEE P7009.1: IEEE Draft Standard for Safety Management of Autonomous and Semi-Autonomous Systems – Interventions in the Event of Anomalous Behavior, [Online:] Available: https://standards.ieee.org/ieee/7009.1/11850/ Accessed 10 July 2026.

[42] IEEE, IEEE 7014-2024: IEEE Standard for Ethical Considerations in Emulated Empathy in Autonomous and Intelligent Systems, [Online:] Available: https://standards.ieee.org/ieee/7014/7648/ Accessed 10 July 2026.

[43] IEEE, IEEE 7014.1-2026: IEEE Recommended Practice for Ethical Considerations of Emulated Empathy in Partner-Based General-Purpose Artificial Intelligence Systems, [Online:] Available: https://standards.ieee.org/ieee/7014.1/11609/ Accessed 10 July 2026.

[44] IEEE, P7017: Recommended Practice for Design-Centered Human-Robot Interaction (HRI) and Governance, [Online:] Available: https://standards.ieee.org/ieee/7017 /11133/. Accessed 16 July 2026.

[45] IEEE Standards Association, P2731 - Standard for a Unified Terminology for Brain-Computer Interfaces, [Online]. Available: https://sagroups.ieee.org/2731/. Accessed: Jul. 16, 2026.

[46] NIST, "Healthcare Standards Testing," [Online]. Available: https://www.nist.gov/itl/products-and-services/healthcare-standards-testing. Accessed: Jul. 16, 2026.

[47] United Nations, "Universal Declaration of Human Rights," 1948.

[48] Council of Europe, "European Convention on Human Rights," 1950.

[49] E. P. Vardas, M. Marketou, and P. E. Vardas, "Medicine, healthcare and the AI Act: gaps, challenges and future implications," European Heart Journal – Digital Health, vol. 6, no. 4, pp. 833–839, Jul. 2025, doi: 10.1093/ehjdh/ztaf041.

[50] WHO news: WHO and HL7 collaborate to support adoption of open interoperability standards, 3 July 2023, [Online] Available: https://www.who.int/news/item/03-07-2023-who-and-hl7-collaborate-to-support-adoption-of-open-interoperability-standards. Accessed 26 July 2026.

[51] J. Mantas et al. "Data Standardization in the Medical Field Through FHIR and FAIR Implementation: A Systematic Review," 2024, [Online] Available: https://journals.sagepub.com/doi/10.3233/SHTI240668 Accessed 26 July 2026.

[52] Digital Health and Informatics Innovations for Sustainable Health Care Systems (Eds.) Data Standardization in the Medical Field Through FHIR and FAIR Implementation: A Systematic Review, 2024

[53] Tejinder Singh Lakhwani, Yerasani Sinjana, Anuj Pal Kapoor, "Revolutionizing healthcare logistics: The strategic role of drone technology in blood bag deliveries for remote and emergency care," Journal of Transport & Health, Volume 42, June 2025, 102053 https://doi.org/10.1016/j.jth.2025.102053

[54] IEEE, IEEE 7010-2020: IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being, [Online] Available: https://standards.ieee.org/ieee/7010/, Accessed 27 July 2026

[55] IEC, IEC 82304-1:2016: Health software — Part 1: General requirements for product safety, [Online] Available: https://www.iec.ch/standards, Accessed 27 July 2026.

[56] ISO/IEC, ISO/IEC 27018:2019: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, [Online] Available: https://www.iso.org/standard/76559.html, Accessed 27 July 2026.

[57] IEEE Standards Association, "IEEE 2621 Certification Program for Medical Device Manufacturers," [Online]. Available: https://standards.ieee.org/products-programs/icap/programs/medical-devices-cybersecurity. Accessed: Jul. 27, 2026.

[58] National Electrical Manufacturers Association, "DICOM Standard PS3.22: Real-Time Communication," DICOM Standard, 2026. [Online] Available: https://dicom.nema.org/medical/dicom/current/output/pdf/part22.pdf Accessed 27 July 2026.

[59] OMOP Common Data Model, Observational Health Data Sciences and Informatics (OHDSI), [Online] Available: https://ohdsi.org/data-standardization/the-common-data-model/, Accessed 27 July 2026.

[60] ETSI, *Smart Body Area Networks (SmartBAN); System Description*, ETSI TR 103 394 V1.1.1, Jan. 2018.

[61] ETSI, Smart Body Area Network (SmartBAN); Low Complexity Medium Access Control (MAC) for SmartBAN, ETSI TS 103 325 V1.1.1, Apr. 2015.

[62] ETSI, Smart Body Area Network (SmartBAN); Enhanced Ultra-Low Power Physical Layer, ETSI TS 103 326 V1.1.1, Jul. 2021.

[63] M. Hämäläinen, H. Iinatti, and A. Toivonen, "ETSI SmartBAN Architecture: The Global Vision for Smart Body Area Networks," *IEEE Access*, vol. 8, pp. 150611–150625, 2020, doi: 10.1109/ACCESS.2020.3016705.

[64] IEEE Standards Association, IEEE 802.15.6-2026: Wireless Body Area Networks (WBANs), [Online] Available: https://standards.ieee.org/, Accessed 27 July 2026.

[65] Toward Dependable Internet of Medical Things: IEEE 802.15.6 Ultra-Wideband Physical Layer Utilizing Superorthogonal Convolutional Code https://pmc.ncbi.nlm.nih.gov/articles/PMC8954192

[66] IEEE 802.15.4j-2013 - IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 4: Alternative Physical Layer Extension to Support Medical Body Area Network (MBAN) Services Operating in the 2360 MHz - 2400 MHz Band https://standards.ieee.org/ieee/802.15.4j/5018

[67] IEC, IEC 62443 (all parts), [Online]. Available: https://www.iec.ch/cyber-security. *Accessed: Jul. 16, 2026.*

[68] X. Chen, Yinchao Yang, N. Fischer, H. Robertshaw, B. Jackson, C. Bergeles, M. Shikh-Bahaei, T. Booth, "Remote Teleoperation of Endovascular Intervention Robots: A Systematic Review," IEEE Transactions on Medical Robotics and Bionics, vol. 8, pp. 579-593, May 2026.

Abbreviations

6G – 6G Communication System

AI — Artificial Intelligence

ML – Machine learning

3GPP – 3rd Generation Partnership Project

ETSI – European telecommunications Standards Institute

UE – User Equipment

GSMA – Global System for Mobile Communications Association

PQC – Post-Quantum Cryptography

ITU-T – International Telecommunication Union – Telecommunication Standardization Sector

LMF – Location Management Function

RAT – Radio Access Technology

MNO – Mobile Network Operator

HMI – Human-Machine-Interface

BCI – Brain-Computer-Interface

AR – Augmented Reality

VR – Virtual reality

QoS – Quality of Service

URLLC – Ultra Reliable Low Latency Communication

MEC – Mobile Edge Computing

ADT — Admission, Discharge, Transfer

Amd — Amendment

AEDs — Automated External Defibrillators

AI Act — Artificial Intelligence Act

AIS — Autonomous and Intelligent Systems

CE — Conformité Européenne

DICOM — Digital Imaging and Communications in Medicine

EHDS — European Health Data Space

EHR — Electronic Health Record

EPR — Electronic Patient Record

EU — European Union

FHIR — Fast Healthcare Interoperability Resources

GDPR — General Data Protection Regulation

HIPAA — Health Insurance Portability and Accountability Act

HL7 — Health Level Seven

HRI — Human-Robot Interaction

IEC — International Electrotechnical Commission

IEEE — Institute of Electrical and Electronics Engineers

IHE — Integrating the Healthcare Enterprise

IMT-2030 — International Mobile Telecommunications-2030

ISAC — Integrated Sensing and Communications

ISO — International Organization for Standardization

ITU-R — International Telecommunication Union Radiocommunication Sector

LLM — Large Language Model

MDR — Medical Device Regulation

NIST — National Institute of Standards and Technology

NHS — National Health Service

ORU — Observation Result (Unsolicited)

ORM — Order Message

P — Draft IEEE standard Project

R4/R5/R6 — FHIR release versions

RTMMS — Radiation Therapy Measurement Management System

SOTIF — Safety Of The Intended Functionality

WG — Working Group

WHO — World Health Organization

XDS — Cross Enterprise Document Sharing