tsdsi
India's Telecom SDO

Telecommunications
Standards Development
Society, India

Whitepaper
May 2026

HEALTHCARE

Enabled by Next-Gen Networks & Technologies

Status, Gaps and Initiatives for Digital Health Ecosystems in India

Important Notice

Individual copies of the present document can be downloaded from www.tsdsi.in Users of the present document should be aware that the document may be subject to revision or change of status.

Copyright Notification

Telecommunications Standards Development Society, India

(TSDSI)

Registered Office Address
C-DOT Campus, Mandi Road,
Mehrauli,
New Delhi, India – 110030
www.tsdsi.in

Foreword

The healthcare sector is undergoing a rapid transformation driven by advancements in next generation networks like 5G and beyond, rapidly evolving IT ecosystem and other enablers such as IoT/IoMT, cloud computing, AI, and immersive digital platforms.

Digital health solutions, connected medical devices, telemedicine platforms, and data-driven healthcare models are reshaping the delivery, accessibility, and management of healthcare services, particularly in geographically remote and underserved regions.

As India advances toward its vision of Viksit Bharat, strengthening healthcare systems through secure, resilient, and inclusive digital infrastructure remains a national priority, supported through initiatives such as Ayushman Bharat and Ayushan Bharat Digital Mission, which emphasize interoperable platforms, trusted communication networks, and scalable digital ecosystems that bridge urban–rural disparities and enhance equitable access to quality healthcare.

This whitepaper identifies systemic gaps, regulatory considerations, and standardization needs required to build secure, interoperable, and future-ready digital healthcare systems.

By providing a deeper assessment of technological enablers, implementation challenges, and policy directions, this document aims to support policymakers, healthcare institutions, telecom operators, service providers, technology developers, and standards bodies in strengthening India's digital health ecosystem through coordinated and standards-driven approaches with citizens as beneficiaries.

Key healthcare applications, including mobile healthcare solutions, Tele-ICU, hospital information systems, clinical trials, mental health and emotional wellbeing, virtual therapeutic interventions, remote workforce skilling Have been outlined the aspects of security, data privacy frameworks, and digital infrastructure with interoperability have been well captured.

The Whitepaper is an outcome of collaborative efforts in a TSDSI forum called TRIP forum.

TSDSI expresses its sincere gratitude to the co-chairs of the TRIP Forum, TSDSI members expert contributors from R&D, academia, and industry; organizations that have implemented pilot projects; and healthcare experts from critical vertical sectors, among others. Despite their demanding schedules, they have generously devoted their time and expertise to contribute to, review, and refine this white paper, with active support from the TSDSI Secretariat. The valuable guidance provided by the TSDSI Roadmap Committee to the TRIP Forum is highly appreciated

We seek suggestions from stakeholders for carrying out further technical studies and development of standards in TSDSI to meet the national requirements for healthcare sector.

A.K Mittal

Director General, TSDSI

Table of Contents

List of Figures

List of Tables

1. List of Abbreviations

Abbreviation	Full Form
ABDM	Ayushman Bharat Digital Mission
ABHA	Ayushman Bharat Health Account
AI	Artificial Intelligence
AR	Augmented Reality
ARTC	Assisted Reproductive Technology Clinic
CBT	Cognitive Behavioural Therapy
CAGR	Compound Annual Growth Rate
C-DAC	Centre for Development of Advanced Computing
CSC	Common Service Centre
CVVH	Continuous Veno-Venous Hemofiltration
DDS	Data Distribution Service
DISHA	Digital Information Security in Healthcare Act
DICOM	Digital Imaging and Communications in Medicine
DPDP	Digital Personal Data Protection
DPDPB	Digital Personal Data Protection Bill
DTLS	Datagram Transport Layer Security
ECG	Electrocardiogram
ECMO	Extracorporeal Membrane Oxygenation
EHR	Electronic Health Record
ETA	Electronic Travelling Aid
GWG	Global Working Group
HaaS	Healthcare-as-a-Service
HD	High Definition
HE	Homomorphic Encryption
HIE	Health Information Exchange
HIMS	Hospital Information and Management System
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HL7	Health Level Seven

HMIS	Hospital Management Information System
HSP	Health Service Provider
ICT	Information and Communication Technology
IPD	In-Patient Department
IoMT	Internet of Medical Things
IoT	Internet of Things
IT	Information Technology
LAN	Local Area Network
ML	Machine Learning
MoHFW	Ministry of Health and Family Welfare
MR	Mixed Reality
MRI	Magnetic Resonance Imaging
M2M	Machine-to-Machine
NIC	National Informatics Centre
NIST	National Institute of Standards and Technology
OPD	Out-Patient Department
PCH	Personal Connected Health
PHR	Personal Health Record
PII	Personally Identifiable Information
PPTTT	Privacy Preserving Techniques Task Team
QoS	Quality of Service
R&D	Research and Development
RFID	Radio Frequency Identification
RIS	Radiology Information System
RPM	Remote Patient Monitoring
SaaS	Software as a Service
SLA	Service Level Agreement
SoC	System-on-Chip
SPDI	Sensitive Personal Data or Information
TLS	Transport Layer Security
TPG	Telemedicine Practice Guidelines

UHI	Unified Health Interface
UHID	Unique Health Identification
UICC	Universal Integrated Circuit Card
UN	United Nations
VR	Virtual Reality
WHO	World Health Organization
Wi-Fi	Wireless Fidelity
XR	Extended Reality

2. Executive Summary

This whitepaper presents a comprehensive view of the evolving digital healthcare ecosystem, with a focus on the integration of advanced communication technologies, next-generation networks, and data-driven solutions. It highlights how emerging capabilities such as Artificial Intelligence (AI), Internet of Medical Things (IoMT), and 5G/6G networks are enabling scalable, efficient, and patient-centric healthcare services.

The study identifies key application domains, including telemedicine, remote patient monitoring, connected medical devices, hospital information systems, and emergency healthcare services. It also examines cross-cutting enablers such as secure digital infrastructure, interoperability frameworks, data governance, and immersive technologies that support advanced healthcare delivery models.

Several critical challenges are outlined, including interoperability gaps, data privacy and security concerns, infrastructure limitations, regulatory fragmentation, and the need for standardized frameworks across stakeholders. The whitepaper emphasizes the importance of aligning national initiatives with global standardization efforts to ensure seamless integration and scalability.

Opportunities are identified in areas such as AI-driven healthcare analytics, real-time monitoring systems, digital twin technologies, immersive healthcare applications, and intelligent automation. These advancements have the potential to significantly enhance healthcare accessibility, operational efficiency, and quality of care, particularly in rural and underserved regions.

Based on these insights, the whitepaper provides recommendations for strengthening standardization efforts, improving interoperability, enhancing data security frameworks, and fostering collaboration between industry, academia, and government bodies. It also highlights the need for a phased and structured approach towards future healthcare systems aligned with next-generation network evolution.

Overall, the whitepaper underscores the importance of a secure, interoperable, and scalable digital healthcare ecosystem in supporting national priorities and enabling inclusive, technology-driven healthcare transformation.

3. Introduction

This whitepaper has been developed as part of the TRIP Forum initiatives under the TSDSI Roadmap Committee, which focuses on domain-specific areas within the broader IoT/M2M ecosystem, including Smart Cities, Healthcare, FinTech, and AgriTech. The healthcare domain has been identified as a critical area due to its increasing reliance on digital technologies and communication networks. The growing need for secure, interoperable, and scalable digital healthcare solutions, along with emerging use cases such as telemedicine, remote patient monitoring, and AI-driven healthcare systems, has motivated the development of this whitepaper.

In this context, the work also aligns with directions from the Department of Telecommunications (DoT). As per GC Action Items GC 33#A5 and GC 37#A06, DoT has requested studies on key verticals to assess digital infrastructure readiness for advanced LTE and 5G use cases, along with the development of strategies for oneM2M interoperability, pilot deployments, and the broader IoT/M2M standards landscape in consultation with TEC.

The healthcare sector is increasingly leveraging digital technologies and communication networks to improve service delivery, accessibility, and quality of care. The convergence of healthcare systems with information and communication technologies (ICT) is enabling new models of care such as telemedicine, remote patient monitoring, connected medical devices, and data-driven healthcare services.

This whitepaper provides an overview of the healthcare ecosystem from a communications and applications perspective, focusing on the role of next-generation networks and digital technologies in enabling emerging healthcare use cases. It highlights key aspects relevant to secure, interoperable, and scalable digital healthcare systems. Artificial Intelligence (AI) acts as a key enabler in this ecosystem, supporting clinical decision-making, diagnostics, and operational efficiency under appropriate regulatory oversight.

The healthcare ecosystem is also evolving towards a Healthcare-as-a-Service (HaaS) model, supported by integrated digital platforms and scalable infrastructure, enabling continuous care across prevention, diagnosis, treatment, and long-term monitoring.

The document is structured to present the objective and scope, followed by healthcare ecosystem aspects covering application domains and cross-cutting enablers. It further discusses regulatory considerations, advanced healthcare delivery models, relevant medical standards, and areas such as medical imaging and remote collaboration. The later sections outline key challenges, emerging opportunities, and recommendations, supported by annexures providing detailed implementation insights.

4. Objective

The whitepaper deals with Remote Healthcare Solutions including telemedicine, management of medical devices, patient management through wearables, exoskeletons, blind stick for divyang, and smart assistive devices for visually impaired & senior citizens, hospital information systems, decision support systems, drug management systems, remote patient monitoring, telesurgery, medical imaging, emergency healthcare for defence personnel and other applications.

Other considerations include security & privacy, digital services infrastructure and architecture, the use of immersive technologies, skill management, regulatory aspects, and references to medical standards for healthcare systems.

The whitepaper also covers aspects related to enhancements required in existing systems, challenges, opportunities, and recommendations for the way forward.

Phase II of the whitepaper will cover deeper analysis of identified use cases, detailed standardization requirements, implementation frameworks, and advanced deployment models, including cross-sector convergence and emerging technologies relevant to future healthcare ecosystems.

The whitepaper deals with Remote Healthcare Solutions including telemedicine, management of medical devices, patient management through wearables, exoskeletons, blind stick for divyang, and smart assistive devices for visually impaired & senior citizens, hospital information systems, decision support systems, drug management systems, remote patient monitoring, telesurgery, medical imaging, emergency healthcare for defence personnel and other applications.

Other considerations include security & privacy, digital services infrastructure and architecture, the use of immersive technologies, skill management, regulatory aspects, and references to medical standards for healthcare systems.

The whitepaper also covers aspects related to enhancements required in existing systems, challenges, opportunities, and recommendations for the way forward.

Phase II of the whitepaper will cover deeper analysis of identified use cases, detailed standardization requirements, implementation frameworks, and advanced deployment models, including cross-sector convergence and emerging technologies relevant to future healthcare ecosystems.

This whitepaper identifies the gaps and opportunities for innovative solutions in aspects of the healthcare sector where communications and application-level implications are involved. In addition, it identifies areas for standardization and examines some of the existing practices in the healthcare services ecosystem.

Disclaimer: The regulatory aspects and their applicability to various geographies are not the focus of this study and need to be independently verified by the reader. This study includes a gap analysis of the healthcare ecosystem, covering existing technologies and standards, and provides recommendations to address identified gaps and support the evolution of digital healthcare systems.

5. Healthcare Ecosystem Aspects

The healthcare ecosystem comprises multiple application domains supported by enabling technologies and cross-cutting system capabilities. Given the breadth of this domain, this section highlights key areas relevant to digital healthcare transformation.

5.1. Core Enabling Technologies

Modern digital healthcare systems are built upon a set of core enabling technologies that collectively support intelligent, secure, and scalable healthcare delivery. These technologies form the foundational architecture for telemedicine, remote monitoring, immersive healthcare, and data-driven clinical decision-making. Key healthcare enabling technologies include:

i. High-Speed Broadband & 5G Connectivity: For low-latency, high-throughput communication enabling tele-ICU, tele-surgery, AR/VR applications, and remote diagnostics.

ii. Cloud Computing & Edge Processing: For scalable data storage, computation, analytics, and distributed healthcare platforms. Internet of Things (IoT) and Internet of Medical Things (IoMT): For real-time patient monitoring, connected medical devices, wearable technologies, and smart hospital infrastructure.

iii. Artificial Intelligence (AI) and Machine Learning (ML): For predictive analytics, clinical decision support, disease diagnosis, population health management, and operational optimization.

iv. Blockchain Technologies: For secure health information exchange, identity management, and improved data integrity across distributed healthcare systems.

v. Security & Privacy Frameworks: Including encryption, authentication, access control, and cybersecurity mechanisms to safeguard sensitive health information.

vi. Interoperability Standards & Unified Platform Architectures: Enabling seamless data exchange across heterogeneous healthcare systems and stakeholders.

Together, these technologies enable integrated, interoperable, and patient-centric healthcare ecosystems aligned with national digital health initiatives.

5.2. Healthcare Application Domains

The following key application domains represent major use cases within the digital healthcare ecosystem:

5.2.1. Mobile Healthcare Solutions

With the advances in data network integration of devices capable of recording patients vital parameters, there is an increasing trend to enable real-time monitoring of patients in emergency scenario. This monitoring enables first responders to take crucial measures in the “golden hour”.

Such an approach is also applicable to telemedicine applications for serving remote patients or cases where physical consultation is not possible.

An important aspect of strategic relevance is the ability to provide telesurgery facility.

It is to be noted that this aspect of Mobile Healthcare Solutions is a dual-use scenario, as it has direct applicability to military personnel well-being and battlefield deployment potential.

5.2.2. Telemedicine

Telemedicine adoption in India has evolved from pilot initiatives to large-scale national deployment. Early efforts led by organizations such as ISRO and C-DAC established connectivity between super-specialty hospitals and remote healthcare centers using satellite-based networks. These initiatives demonstrated the feasibility of remote consultations, teleradiology, and tele-education in geographically challenging regions.

In recent years, telemedicine has transitioned from experimental deployment to structured digital health integration under national programs. The launch of platforms such as eSanjeevani under the Ministry of Health and Family Welfare, along with initiatives under the Ayushman Bharat Digital Mission (ABDM), has enabled scalable teleconsultation services across states and union territories.

The COVID-19 pandemic significantly accelerated telehealth adoption, leading to rapid expansion of teleconsultation, e-pharmacy, remote diagnostics, and virtual follow-up services. Telemedicine is now recognized as a long-term component of India's digital health strategy rather than a temporary emergency solution.

Government programs such as the National Medical College Network, BharatNet, National Health Stack, and SATCOM-based connectivity initiatives further support integration of telemedicine into mainstream healthcare delivery.

5.2.2.1. Telemedicine Solutions

The evolution of telemedicine is enabling the development of a connected healthcare ecosystem, where patients, providers, medical devices, and emergency services are seamlessly integrated through high-speed communication networks. This ecosystem extends beyond traditional virtual consultations and supports real-time collaboration across distributed healthcare environments.

This rapid transition demonstrated the scalability, accessibility, and long-term viability of telemedicine platforms, leading to sustained integration of virtual care models beyond the pandemic period.

Key elements of a connected healthcare ecosystem include:

i. Connected Ambulances: Ambulances equipped with medical devices and communication systems that transmit patient vitals, imaging, and clinical data in real-time to hospitals during transit, enabling early intervention.

ii. High-Definition (HD) Virtual Consultations: Secure, high-quality video platforms that support remote specialist consultations, tele-ICU services, and collaborative diagnosis.

iii. Remote Monitoring and Servicing of Medical Equipment: Centralized hubs enabling remote diagnostics, monitoring, and maintenance of hospital equipment to improve operational efficiency.

iv. Video-Enabled Medication Adherence: Digital platforms that support supervised medication intake, particularly for chronic disease management and public health programs.

v. Edge Processing and Real-Time Throughput: Use of edge computing and high-bandwidth networks to process clinical data locally, reduce latency, and support time-critical healthcare applications.

This integrated digital healthcare model strengthens care continuity, improves access in rural and underserved areas, enhances clinical decision-making, and supports scalable, technology-driven healthcare delivery models.

Multilingual support and regional language enablement are critical for inclusive digital healthcare adoption. Voice-enabled interfaces, vernacular teleconsultation platforms, and speech-to-text tools in regional languages can significantly improve healthcare accessibility for economically weaker and semi-literate populations, particularly in rural and remote regions

Note: Detailed state-wise deployments and institutional networks are provided in Annexure I.

5.2.2.2. Remote patient monitoring

Remote Patient Monitoring (RPM) enables continuous collection and transmission of patient health data for timely clinical assessment and intervention. It supports proactive and preventive healthcare by enabling real-time monitoring outside traditional clinical settings.

RPM is widely used for chronic disease management, elderly care, post-operative monitoring, and home-based healthcare services. It reduces hospital visits and improves patient outcomes through early detection and timely intervention.

The key components of RPM solution are described below:

i. Sensors: Medical and wearable sensors are used to capture patient vitals and physiological parameters such as heart rate, blood pressure, oxygen saturation, glucose levels, and body temperature.

ii. Local Storage: Collected data may be temporarily stored on patient-side devices or gateways to ensure reliability during intermittent connectivity and support data buffering.

iii. Connectivity: Data is transmitted using communication technologies such as Bluetooth, Wi-Fi, and telecom networks (4G/5G), enabling secure and real-time data transfer from patient devices to healthcare systems.

iv. Central Repository: A centralized data repository or cloud platform stores patient data securely, supporting longitudinal health records, analytics, and integration with other healthcare systems through standard interfaces.

v. Diagnostic and Monitoring Software: Clinical dashboards and analytics software process incoming data to generate alerts, trends, and insights for healthcare providers, enabling timely decision-making and continuity of care.

This layered architecture, supported by M2M communication frameworks, enables scalable, interoperable, and efficient remote patient monitoring.

Integration of edge computing within RPM architectures further enhances real-time analytics and reduces latency, particularly in emergency and chronic disease management scenarios. Edge-enabled monitoring ensures continuity of care even in low-bandwidth environments.

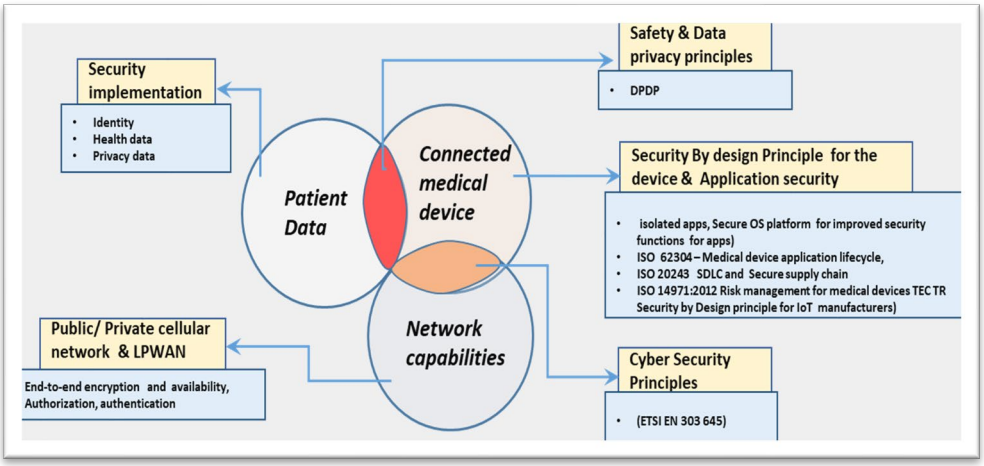
Note: Illustrative implementations and deployment models related to telemedicine and remote healthcare solutions are provided in the Annexure III to Annexure X

5.2.3. Medical Devices

Increasing connectivity and rapid growth of medical devices, and even hybrid wireless technologies, are creating challenges related to device security and data privacy. Various incidents have been reported involving exposed vulnerable devices and software applications. Considering the potential impact on clinical care, patient safety, and privacy, there is a need to protect medical devices and patient data from the cyber-attacks.

The figure 1 illustrates the key area for strengthening device security and data protection in connected medical devices.

FIGURE 1: SECURITY CONSIDERATIONS AND DATA PROTECTION REQUIREMENTS FOR CONNECTED MEDICAL DEVICE



5.2.4. IoT and IoMT for Patients

While the Internet of Things (IoT) broadly refers to interconnected smart devices across various industries, the Internet of Medical Things (IoMT) represents its healthcare-specific subset. IoMT focuses exclusively on connected medical devices, clinical systems, and patient monitoring applications designed to collect, transmit, and analyse health-related data within regulated healthcare environments.

5.2.4.1. IoT for Patients – Smart Assistive Device for Visually Impaired

a. Smart Assistive Wearable System (Smart Jacket & Smart Cane)

The proposed system is an Electronic Travelling Aid (ETA) designed as a wearable smart assistive solution for visually impaired and elderly individuals. The system comprises two integrated components:

i. A Smart Jacket (wearable control unit)

ii. A Smart White Cane

The solution leverages IoMT architecture, embedded sensing, real-time processing, and wireless communication technologies to enhance mobility, safety, and independence.

b. System Architecture Overview

The Smart Jacket is built on a compact System-on-Chip (SoC) platform integrated

with:

i. Ultrasonic sensors for obstacle detection

ii. GPS module for tracking location

iii. Motion and orientation sensors

iv. Audio output interface (wired/wireless)

v. Control comprises the jacket

The Smart White Cane complements the jacket by enabling environmental sensing at ground level, particularly for wet surfaces and pothole detection.

The system processes environmental inputs in real-time and provides immediate voice-based alerts to the user in multiple languages.

c. Functional Capabilities

The Smart Assistive System supports the following core features:

i. Obstacle Detection & Distance Estimation: Identifies objects in the user's path and estimates their distance.

ii. Object Height Detection: Assists in identifying overhead or mid-level obstacles.

iii. Emergency Alert Services: Enables one-touch emergency notifications to predefined contacts and services.

iv. GPS-Based Location Sharing: Captures latitude and longitude coordinates and generates shareable location links.

v. On-Demand Cab Booking Support: Enables users to book a cab through a single-touch interface using real-time GPS location sharing.

vi. Wet Surface & Water-Filled Pothole Detection: Alerts users to prevent slipping hazards.

vii. Cane Relocation Assistance: Provides audio cues if the user loses contact with the cane.

This architecture ensures real-time sensing, processing, and user alerting through embedded control modules.

d. Functional Objectives of Smart Assistive Wearable Devices

i. To design a portable and wearable device for visually impaired individuals to assist them in navigation, alert the user to obstacles in their path and detect surrounded objects and calculate their distance from the user.

ii. To determine the approximate height of surrounding objects.

iii. To enable the person to book a cab with a single touch and provide the option to share their location with relative or emergency service.

iv. To convert system instructions into voice signals that can be delivered to the visually impaired person.

v. To design a smart cane that alerts the user about wet surfaces, helping prevent slipping, and also assist in relocating the cane if it is misplaced.

e. Overall Function of Smart Assistive Wearable Devices

i. Alert users about obstacles while walking.

ii. Alert the user regarding the height of surrounded obstacles.

iii. Capture the user's location using GPS and use it to book a taxi.

iv. Share the user's location with relatives and emergency services, such as ambulance and police, in case of an emergency.

v. Alert the user about wet floors and water filled potholes filled to prevent slipping.

FIGURE 2(A): DESIGN OF JACKET

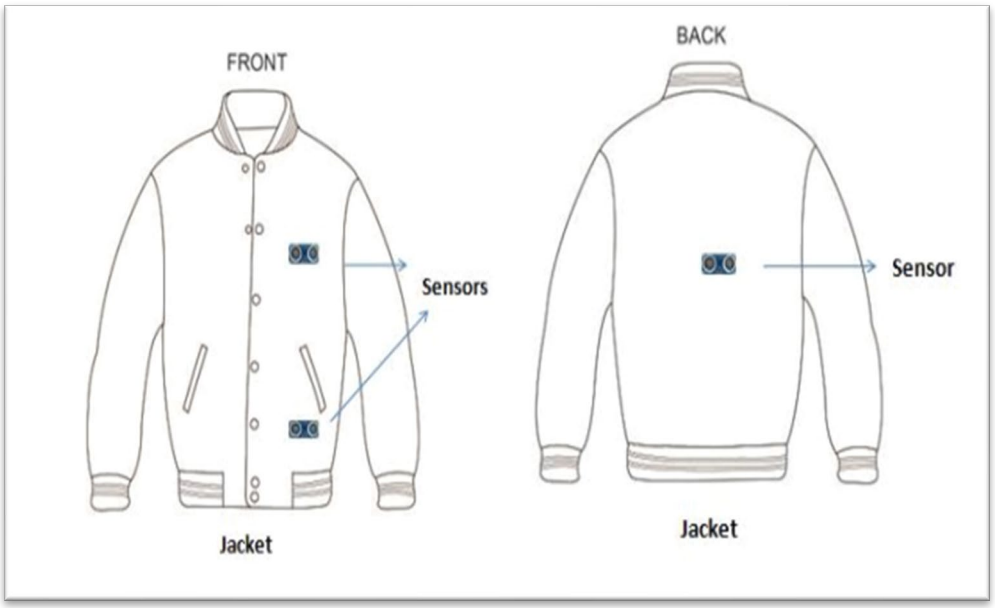


FIGURE 2(B): DESIGN OF JACKET

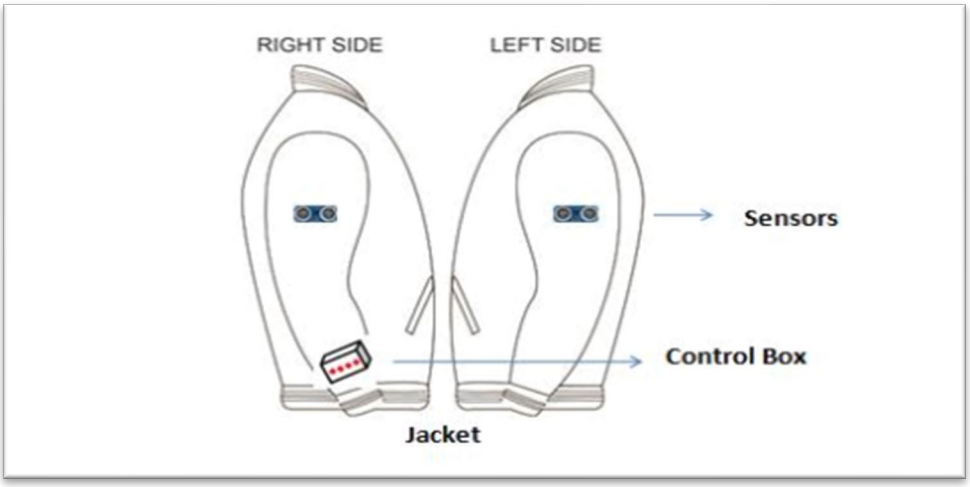
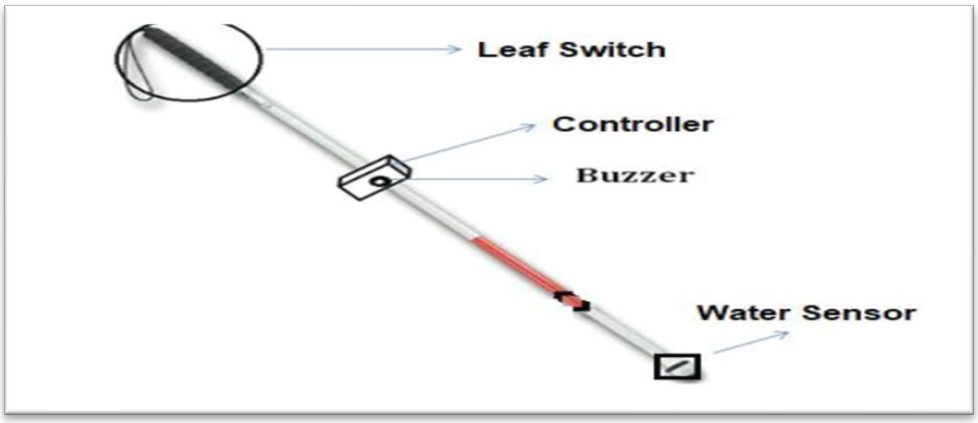


FIGURE 3: SMART CANE



f. Use of Artificial Intelligence in Smart Assistive Wearable Devices

To enhance the intelligence of the smart jacket and smart cane, artificial intelligence (AI) capabilities can be integrated. The following features may be incorporated in future enhancements:

i. Identification of bus stops, train platforms, seating locations, bus doors and handles.

ii. Detection of wet floors to enhance safety and prevent slipping.

iii. Reading signs and text, allowing the device to read aloud information from signs, labels, and printed materials.

iv. Product identification, enabling users to scan and recognize products in retail environments.

v. Face recognition, allowing identification of known individuals to support social interaction.

vi. Support during social interactions, by providing contextual information about nearby people and activities.

g. Use of 5G in Smart Assistive Wearable Devices

i. High-speed 5G connectivity enables real-time information exchange with cloud servers, thereby improving device accuracy and reducing response latency.

ii. The smart stick can utilize 5G connectivity to transmit sensor data to the cloud for rapid processing, enabling advanced obstacle detection algorithms that consider complex environmental factors.

iii. Improved navigation is enabled through low-latency, real-time turn-by-turn guidance, particularly in dynamic or complex environments.

iv. Cloud-based AI access through 5G allows the smart stick to leverage advanced image recognition and object detection algorithms.

v. Augmented reality (AR) integration with smart glasses or smartphones can overlay navigational and object information, enhancing user awareness.

vi. Remote assistance is supported through low-latency video communication, enabling sighted assistants to provide real-time guidance.

vii. Emergency services integration allows the device to automatically contact emergency responders and transmit precise location information, enabling faster assistance.

Note: Technical hardware specifications and component-level details are provided in Annexure II.

5.2.4.2. Internet of Medical Things (IoMT) for Patients

The Internet of Medical Things (IoMT) refers to the ecosystem of interconnected medical devices, sensors, software applications, and healthcare systems that collect, transmit, and analyse patient health data over secure communication networks. IoMT enables real-time monitoring, remote diagnostics, and continuous care delivery by linking patients, healthcare providers, and medical infrastructure through digital platforms.

IoMT serves as a key enabler of personalized, preventive, and data-driven healthcare.

a. Types of IoMT Devices

IoMT devices can be broadly categorized as follows:

i. Wearable Devices: Smartwatches, ECG monitors, glucose monitors, pulse oximeters, and fitness trackers used for continuous monitoring of vital parameters.

ii. Remote Patient Monitoring (RPM) Devices: Home-based monitoring systems for chronic disease management.

iii. Smart Implants and Connected Therapeutic Devices: Pacemakers, smart inhalers, insulin pumps, and ingestible sensors.

iv. In-Hospital IoMT Systems: Smart beds, infusion pumps, asset tracking systems, RFID-enabled equipment, and diagnostic imaging devices.

v. Connected Emergency Systems: Ambulance-based monitoring systems transmitting patient data to hospitals in real time.

b. Benefits of IoMT

i. Supports integration with remote patient monitoring systems and enhances data-driven healthcare delivery.

ii. Improves accessibility to healthcare services, especially in rural and underserved areas.

iii. Enhances clinical decision-making through real-time data availability.

iv. Supports preventive and personalized care models.

v. Optimizes hospital operations through asset tracking and workflow management.

c. Challenges of IoMT

i. Security and Privacy Risks: Increased exposure of sensitive health data to cyber threats.

ii. Interoperability Issues: Lack of uniform standards across devices and platforms.

iii. Data Ownership and Governance Concerns: Clarity required regarding data access and usage rights.

iv. Infrastructure and Cost Constraints: Upfront deployment costs and dependency on reliable broadband connectivity.

5.2.4.3. Societal Impact

This solution demonstrates how IoMT, AI, and next-generation communication networks can enable inclusive, patient-centric assistive healthcare technologies. It supports digital empowerment, enhances safety, and improves quality of life for vulnerable populations.

5.2.4.4. M2M Framework for Remote Health Monitoring

Machine-to-Machine (M2M) communication enables a Personal Connected Health (PCH) ecosystem where wearable devices and medical sensors continuously capture vital parameters and transmit them to healthcare providers. In a typical architecture, patient devices collect physiological data (e.g., heart rate, SpO_2, glucose levels, blood pressure), which is transmitted via Bluetooth or similar short-range technologies to a smartphone or local gateway. The data is then forwarded through Wi-Fi or telecom networks to centralized repositories or cloud platforms for clinical analysis.

This M2M-enabled framework supports remote patient monitoring by enabling seamless data acquisition, transmission, and clinical integration across healthcare systems.

5.2.5. Hospital Information Systems (HIS)

Traditional Hospital Information Systems (HIS) have been monolithic in design, with a single application catering to multiple functional domains. Where required, Institutions would purchase/develop those modules that they did not obtain in the first iteration. Often, this entailed searching and acquiring “best of breed” systems, followed by integration at

different levels into the existing HIS with its accompanying challenges and opportunities. Although this helped mitigate capital expenditure, it often resulted in a haphazard collection of various applications of differing vintage and platforms.

Keeping the applications and backend system synchronized became a significant challenge, with each application having its own lifecycle management, support, upgrade and end-user training requirements. Most traditional systems operated on on-premises hardware and servers, resulting in challenges related to continuity, security, upgrades, and access control.

The modern approach has been to implement solutions that have capacity to extend across most functional domains, are modular in nature, and can be implemented with minimum disruption, as the underlying platform (database, front-end, application model etc.) remains largely consistent. This approach also enables better planning and management of capital expenditure. The availability of cloud-based solutions offers improved control over capital costs, distributed access, and enhanced scalability, although long-term benefits at a large scale in the Indian context are yet to be fully documented.

5.2.5.1. Challenges in Hospital Information Systems

i. Lack of licensing requirements for mandated standardization.
ii. Non-adherence to international and national standards
iii. Absence of interoperability, except when the same application is used within a single organization, due to non-adoption of standards related to vocabulary, codes, messaging.
iv. Lack of comprehensive data protection regulations, both general and healthcare specific.
v. Limited awareness of policy and framework requirements that should be addressed prior to software implementation.
vi. Absence of a standard authentication mechanism for patients, healthcare workers, and healthcare facilities.
vii. High costs associated with hardware acquisition, maintenance, upgrades, and disposal, compounded by early obsolescence.
viii. High costs of software lifecycle management, including support and upgrade charges.
ix. Impact of system costs on overall healthcare costs borne by patients.
x. Connectivity challenges, including the lack of reliable, low-cost, and secure communication networks within and between healthcare facilities.
xi. The clinician–computer interface remains largely limited to keyboard and mouse, with some applications using touch panels, requiring significant improvement.
xii. Diverse user requirements across patients, clinical teams, and financial operations necessitate human-readable narrative reports; while reporting and analytics require structured, coded data, which is difficult to acquire. Data authentication and cleanliness remain challenges due to flexible workflows and editable free text, often mimicking paper-based health records.
xiii. Patient communication systems that support secure, convenient, and multi-modal information exchange are required. The multiplicity of platforms and authentication mechanisms introduces additional challenges, including confidentiality and privacy concerns.

xiv. Use of publicly available communication platforms for clinical purposes without adequate consideration of security, privacy, confidentiality, and medico-legal implications.

xv. Proprietary data platforms used by medical device vendors for data acquisition, storage, and transmission, leading to interface challenges and high transition costs when migrating legacy data to new systems.

xvi. IoT connectivity challenges, including the absence of frameworks, messaging standards, and content standards, as well as issues related to data sharing and confidentiality. This includes distinctions between device monitoring data for manufacturers and clinical or diagnostic data shared with healthcare stakeholders.

xvii. Variations in IT literacy and penetration across the population, limiting uniform implementation of digital health systems.

xviii. Within healthcare facilities, inadequate hardware infrastructure for real-time data collection and workflow management, leading to reliance on data entry operators.

xix. Absence of a recognized national forum for academic or research-based discussion of these issues, including the creation of interoperable research data warehouses. Most research efforts are currently vendor-driven.

xx. Responsible exploration of data usage for the development of AI-enabled systems to support diagnosis, care delivery, monitoring, and clinical documentation.

5.3. End-to-end Enablers

These end -to-end enablers support multiple healthcare application domains and are critical for ensuring secure, reliable, and scalable system operation. This section outlines the key technological enablers that support secure, scalable, and interoperable digital healthcare systems, including security and privacy frameworks, 5G connectivity, digital infrastructure, and emerging technologies.

5.3.1. Security and Data Privacy

Security issues in healthcare data are a significant concern due to the sensitive nature of the information and the potential consequences of data breaches. Recent attacks on medical data have highlighted significant vulnerabilities in healthcare systems. One notable incident involves Change Healthcare, which experienced a cyberattack impacting numerous hospitals, doctors, and pharmacies across the United States. This attack resulted in disruptions to claims processing and payments, affecting cash flow for many providers (American Hospital Association). In another instance, ransomware attacks by groups like Black Basta have increased, targeting healthcare facilities and compromising patient data. These attacks can lead to significant operational disruptions, delays in patient care, and potential financial losses.

These incidents underscore the critical need for robust cybersecurity measures in healthcare to protect sensitive patient information and ensure continuity of care.

There have been new initiatives in India for a robust cybersecurity framework after a major ransomware attack on health data.

5.3.1.1. Key Security Challenges

The key security challenges related to healthcare data are discussed below:

i. Data Theft: Healthcare data includes highly sensitive information such as patient medical histories, treatment plans, and personal identification details. The vulnerability, mishandling, or misconfiguration of the storage of the health data can create serious consequences. The unauthorized access or theft of the data can lead to identity theft and other malicious activities. Sometimes the payment information associated with healthcare services can also be targeted, leading to financial fraud and loss. If data stored on servers or devices is not encrypted, it is vulnerable to theft and unauthorized access. Unencrypted data transmitted over networks can be intercepted by attackers, leading to potential breaches.

ii. Ransomware Attacks: Attackers may encrypt patient data, demanding a ransom to restore access. This can disrupt healthcare services and put patients at risk. Ransomware can incapacitate healthcare systems, delaying treatment and affecting patient care. The availability of the data or health service may be disrupted due to these types of ransomware attacks.

iii. Failure in Access Control: Weak authentication mechanisms (e.g., simple passwords, shared accounts) can allow unauthorized individuals to access sensitive data.

Insufficiently controlled user privileges can enable users to access data beyond their authorization.

iv. Vulnerabilities in Medical Devices: Connected medical devices may have vulnerabilities that may have been retained after manufacturing or first level testing which can be exploited to access patient data or disrupt device functionality. Outdated or unpatched software in medical devices can be targeted by attackers.

v. Third-Party Risks: Third-party service providers and partners who handle healthcare data may have weaker security measures, creating additional risk. Data Sharing with external organizations, even after formal agreements, may pose risks of unauthorized access and breaches if not properly managed.

vi. Data Integrity Issues: Unauthorized modification of healthcare data can lead to incorrect diagnoses, treatment errors, and harm to patients. Human errors or software glitches can also result in unintended changes to patient records.

5.3.1.2. Security Mitigation Strategies

Several mitigation strategies are implemented to address these issues and vulnerabilities in healthcare devices and data system. The current defence mechanisms and methodologies are listed below.

i. Strong Encryption: Encrypt data both at rest and in transit to protect it from unauthorized access.

ii. Enforce Strict Access Controls: Use multi-factor authentication and role-based access controls to limit access to sensitive data.

iii. Regular Security Audits: Conduct frequent security assessments and vulnerability scans to identify and address potential weaknesses.

iv. Employee Training: Educate staff on cybersecurity best practices and the importance of data protection.

v. Update and Patch Systems: Regularly update software and firmware to address known vulnerabilities.

vi. Incident Response Planning: Develop and test incident response plans to quickly and effectively respond to data breaches and security incidents.

vii. Deploy Intrusion Detection Systems: Utilize advanced security systems to detect and prevent unauthorized access and modifications to medical records.

viii. Maintain Backups: Regularly back up medical records to secure, immutable storage to restore data in case of tampering.

By addressing these security issues with appropriate measures and vigilance, healthcare organizations can better protect their sensitive data and maintain the trust of their patients.

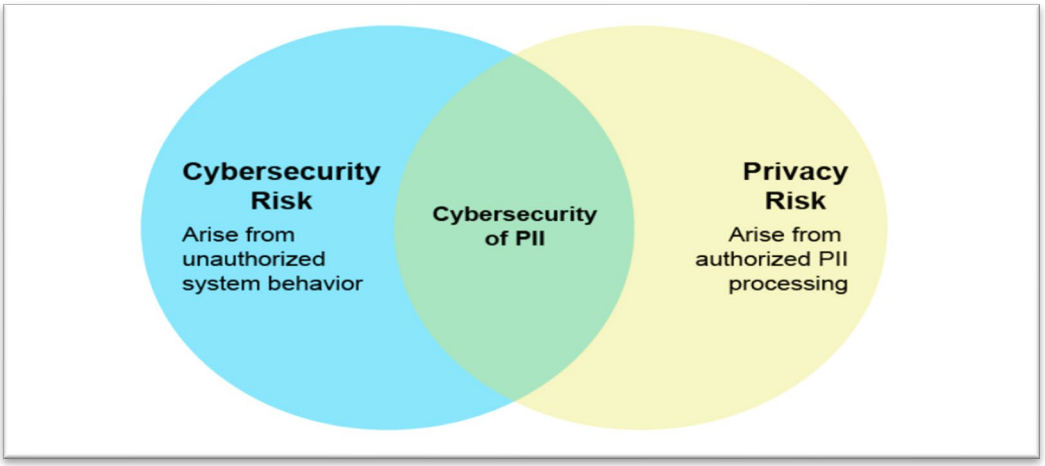
5.3.1.3. Data Privacy Challenges and Mitigation Measures

Patient data privacy is another challenge related to the safety and privacy of patients. The implementation of data sharing or authorization should be based on approval of the custodian only who owns the device. Patient devices should be secured using encryption methods at the firmware level or through tamper-proof hardware components, such as secure element or UICC/eUICC.

The logical implementation in such a way that custodian of device can grant privilege to authorised individuals who require patient data for analysis or for clinical purpose. The privilege holder should only be able to access patient information from the controller server or patient platform. The shared privilege should be time-bound, after which the access privilege should be expire.

Identity theft is directly related to individual privacy, and the security of IoT devices revolve around the protection of personally identifiable information (PII). There are three layers to secure an individual privacy in IoT devices for the health sector: disassociated data management, informed decision making and PII processing permissions management. The relationship of privacy risk and PII management system in IoT environment can be understood form the following illustration.

FIGURE 4: CYBERSECURITY OF PII AND RISKS



The IoT devices in the health sector are a major source of personally identifiable information (PII), and the data privacy regulations are strictly applicable from the initial stage to the final stage of IoT device operation. The main concern for the PII is its security during process. PII may be processed in ways that are non-compliant with regulatory requirements or an organization's policies. IoT devices may be complex and dynamic, with sensing functionality that can collect PII being frequently added and removed therefore, a well-established update and notification mechanism for obtaining user consent is essential for the PII getting from the of IoT device communication.

The available privacy-preserving techniques are in the research and development (R&D) phase to address data security challenges when data is available in encrypted form during process.

The push of digital health infrastructure through the Ayushman Bharat Digital mission has started, and multiple R&D activities are underway globally to protect data privacy. The Privacy Preserving Techniques Task Team (PPTTT) is advising the UN Global Working Group (GWG) on Big Data on developing the data policy framework for governance and information management of the global platform, specifically to support privacy-preserving techniques. However, there are no clear guidelines in India for specifying health-sector data classification based on privacy concerns.

Genomic repositories are one of the sources where specific guidelines for privacy protection are required. i2b2 and tranSMART were developed to provide clinical and translational investigators with the tools necessary to integrate medical records and clinical research data in the genomics era. Privacy-preserving techniques based on Homomorphic encryption (HE) and their application have been widely applied in medical and health sector IoT devices. However, clear guidelines for HE-based inclusion in healthcare IoT devices are still evolving.

The data lifecycle is another challenge in terms of data privacy. Questions related to how long patient data is stored in data centre and the guidelines for deletion fall under the concepts of the “right to erasure” or “right to be forgotten.” In the health sector, data collection is not always digital; at the primary level, it is often physical and later converted into digital form based on processing requirements. Therefore, the process of deleting health-related data requires clearly defined frameworks.

One of the emerging markets in the health sector in our country is assisted reproductive technology clinic (ARTCs). This is an area where recent judgments in the United States have influenced policies related to data deletion and embryo management. These aspects are not addressed in the Assisted Reproductive Technology Regulation Bill (2020).

The NIST publication “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks” provides several suggestions and recommendations for IoT devices security in health sector specific applications. The potential cybersecurity challenges are elaborated in the NIST document through three goals:

Goal 1: Protect device security

Goal 2: Protect data security

Goal 3: protect individual privacy

Goal 2 and 3 are the primary concern for health-related IoT applications. The alteration of private health data can trigger multiple security threats. An attacker who merely views stored or transmitted IoT data may gain limited value; however, an attacker who alters the data can initiate a chain of events leading to serious incidents.

There are three expectations listed in terms of the protection of data security in IoT devices, covering data at rest, in transit, and during processing:

i. The device can prevent unauthorized access to all sensitive data on its storage devices.

ii. The device has a mechanism to support data availability through secure backups.

iii. The device can prevent unauthorized access to all sensitive data transmitted from it over networks.

The first expectation is targeting those IoT devices which do not have sufficient encryption mechanisms for transmitting as well as storing data. Unavailability of a mechanism for sanitizing sensitive data before disposing of or repurposing a device is another threat for data security in IoT devices. An IoT device may fail to verify the identity of another computing device before sending sensitive data over its network communications, and this requirement is addressed in the third expectation listed in the NIST document. Transport Layer Security (TLS) provides the key security benefits such as encryption, data integrity, authentication, and secure connectivity for IoT device communications.

The main points of data security are:

i. Confidentiality: Information should not be disclosed to unauthorised users, devices or software.

ii. Integrity: It should be ensured that once data is created, it is not altered.

iii. Availability: It should be ensured that data and resources are accessible to authorized users whenever required.

iv. Authenticity: Designed to establish the identity of a transmission, message, or originator.

v. Access Control: Enables mechanisms through which an authority controls access to resources in a physical facility or online information system.

Typically, TLS/ DTLS or DDS security is used.

5.3.1.4. TLS (Transport Layer Security) / DTLS (Datagram Transport Layer Security)

These are used in most middleware systems to ensure data security. They provide secure communication over a network and are cryptographic protocols. TLS is designed for stream-oriented connections, while DTLS is designed for datagram-based connections. TLS achieves some level of availability due to the reliability of TCP.

Both TLS and DTLS provide a high level of confidentiality, integrity, and authenticity. TLS achieves availability due to TCP reliability, while DTLS lacks inherent availability mechanisms as it operates over UDP. Both are state-of-the-art mechanisms with a channel-centric approach to confidentiality, integrity, and authenticity. However, both TLS and DTLS lack granular, data-centric access control mechanisms, and access control is not addressed within these protocols.

5.3.1.5. DDS (Data Distribution Service) Security

This standard is based on a data-centric, publish–subscribe communication approach. Its decentralized architecture provides low latency and high reliability. DDS security, when combined with Quality of Service (QoS), forms a powerful communication framework that can be adapted to user requirements.

DDS security provides a fine-grained, data-centric approach to confidentiality, integrity, and authenticity. Access control is achieved through granular, data-centric security overlays. High availability is supported through decentralized architecture, extensive QoS features, and reliable communication, providing an additional level of security.

5.3.2. Role of 5G in Healthcare Systems

5.3.2.1. Healthcare Use Cases for 5G Network Slicing

The healthcare industry can greatly benefit from the implementation of 5G technology, which offers enhanced mobile broadband, ultra-reliable and low-latency communication, and massive machine-to-machine communication capabilities. Private 5G networks in healthcare can be used to provide secure, high-speed communication and data transfer within hospitals or other healthcare facilities. This can facilitate real-time communication and collaboration between medical staff and improve the accuracy and efficiency of medical procedures. Public 5G networks in healthcare can be used to provide remote patient monitoring and telemedicine services to individuals in underserved or remote areas, connected ambulances, and remote robotic-assisted surgery.

While the potential benefits of 5G technology in healthcare are widely acknowledged, there are several barriers to its widespread adoption. These include a lack of research and academic literature, limited demonstration of practical use cases, and the involvement of multiple parties with competing interests, such as modality OEMs, healthcare professionals, internal hospital infrastructure, private 5G OEMs and service providers, and public 5G service providers. As a result, hospitals lack a clear vision and roadmap for investment in 5G technology, making it challenging to fully capitalize on its potential to improve patient care and outcomes.

To effectively leverage 5G technology in healthcare, there is a need to identify and evaluate practical use cases, implement changes to medical modalities to support these use cases, and establish standard network service-level agreements (SLAs) for various applications. It is also important not only to identify and evaluate use cases but to demonstrate them in real-world scenarios. This may include pilot projects and testing in operational healthcare facilities, which can provide valuable insights into implementation feasibility and effectiveness.

5.3.2.2. Healthcare Use Cases Requiring 5G Connectivity

This section lists some generic use-cases in the healthcare space that potentially cover the full range of network requirements.

There are numerous use-cases across modalities that can benefit from the capabilities of 5G. The table below provides a holistic view of such use cases, mapped against the key capabilities of 5G.

TABLE 1: MAPPING OF HEALTHCARE USE CASES TO KEY 5G CONNECTIVITY REQUIREMENTS

Use case	Low Latency	High Bandwidth	Mobility	Reliability & Security	Capacity	Private 5G only
Connected ambulance	√	√	√	√		
HD virtual consultations		√	√	√		

Remote patient monitoring (tele-ICU, tele-radiology)	√	√	√	√	√	
Video-enabled medication adherence		√		√		
Remote access to asset (machine data) and remote servicing of hospital equipment Remote operation of the equipment from a central hub	√	√		√		
AR/VR use cases for palliative care/ Training & education	√	√	√	√		√
Remote robotic surgery	√	√		√		
Real time high throughput Edge processing	√	√	√			√

The combination of 5G connectivity and edge computing provides a robust framework for time-critical healthcare applications requiring ultra-low latency, high reliability, and localized intelligence.

In the case of a medium / large hospital, many of these use-cases occur simultaneously. This clearly calls out the need for standardization in the following areas:

i. A specific network slice for healthcare (HC) data in general
ii. In a given hospital network, dynamic allocation of network slices.
iii. In a mobility case, the hand-over from public 5G slice to a private 5G in a hospital.

Use case 1: Tele Radiology

High speed uplink and downlink capability of 5G network enables radiologists to exchange large, scanned images of patients (DICOM files) in a fairly quick time for remote processing to an edge or Cloud computing service equipped with AI/ML capabilities for enhanced and more accurate diagnostics, or to another facility for expert opinion.

Use case 2: Tele Medicine & Remote patient monitoring

A high-bandwidth and low-latency 5G network immensely augments the scope of telemedicine and remote patient monitoring solution by enabling following use cases:

i. Smart ICU with 5G-enabled depth camera along with patient body sensors.
ii. Connected ambulance.
iii. Touch free OPD / Ward visit.

Use case 3: Tele-ICU

Eighty percent of physicians in India work in urban areas, while 70% of the population resides in remote locations that suffer from a severe shortage of doctors and trained intensivists. This imbalance in critical care availability is associated with high costs and increased morbidity and mortality. Building high-acuity intensive care units (ICUs) in remote locations is typically not feasible due to lack of funding, technology, and staffing resources. On the other hand, transferring an acutely ill patient over a long distance to a well-equipped urban ICU is both time-consuming and risky.

A viable model to overcome these access challenges is the concept of tele-ICU, which uses a network of audio-visual and patient surveillance systems to link a critical-care team of nurses, doctors, and intensivists from a remote hospital to the resources of a large multi-specialty facility. It enables delivery of immediate, standardized care to critically ill patients, increases accessibility to intensive care, and supports efficient utilization of limited resources.

Use case 4: Data acquisition of asset data to monitor and service healthcare equipment.

Ability to acquire high-frequency asset data from sensors or machine logs to analyze machine and asset health remotely and proactively plan maintenance.

5.3.2.3. Need for a Dedicated Healthcare Network Slice

Network slicing is a 5G technology that allows for the creation of multiple virtual networks on top of a single physical network infrastructure and plays a major role in defining service-level agreements. For example, a network slice can be dedicated to telemedicine, ensuring that the necessary bandwidth and low latency are allocated for real-time video conferencing between patients and doctors. Another slice can be dedicated to remote surgery, providing the ultra-reliable and low-latency communication required for accurate control of robotic surgical tools. This can help to improve the quality and responsiveness of healthcare services while also providing the security and privacy required to protect sensitive patient data.

A Service Level Agreement (SLA) for network slicing in healthcare defines the quality of service (QoS) that will be provided for each slice of the network. It outlines the key performance indicators (KPIs) and metrics that will be used to measure the performance of the network slices, as well as the targets that comply with the SLA.

5.3.3. Digital Infrastructure and Platforms

Digital health requires a robust, reliable, and secure digital infrastructure to support its various functions. Essential components of digital infrastructure that are necessary for practicing digital health are:

i. Electronic Health Records: Electronic Health Records (EHRs) are digital records of a patient's medical history, including diagnosis, treatment, medications, radiology scans and pathology test results. They organize patient’s health information and make it universally accessible and useful.

ii. Communication Networks: High-speed networks are required to transmit and exchange medical images like CT scan and MRI images. For this, hospitals need to implement high-speed LAN infrastructure (10G backbone and 1G access network) and Wi-Fi (Wi-Fi 6) infrastructure. There is often a requirement to provide healthcare services in remote areas which do not have good physical healthcare infrastructure. 5G/4G mobile data connectivity can be used to provide connectivity in such remote areas.

iii. Health Information Exchange: Health Information Exchange (HIE) enables secure sharing of patient health information between healthcare providers, regardless of the EHR system they use. HIE helps healthcare providers access and share patient information securely and efficiently using HL7 (version 2.x) message exchange, thereby improving patient care and coordination. Interoperability requires computable, machine-readable implementation guides and automated conformance validation frameworks to reduce ambiguity and ensure consistent interpretation across healthcare systems. Adoption of well-defined message profiles and structured conformance mechanisms reduces ambiguity in data exchange and significantly improves interoperability across heterogeneous healthcare systems.

iv. Patient Portals: Patient portals are secure web-based platforms that allow patients to access their medical records, schedule appointments, communicate with their healthcare providers, and manage their health. In hospitals, these portals are implemented as a part of the Hospital Information and Management System (HIMS).

v. Mobile Health Apps: Mobile health apps are smartphone applications that provide patients with tools to monitor and manage their health, such as tracking their medications, monitoring their vitals and symptoms, and receiving health education.

vi. Telehealth Platforms: Telehealth platforms enable remote patient consultations, monitoring, and treatment through video conferencing, remote monitoring, and other digital tools.

vii. Decision Support Systems: These are software tools that provide healthcare providers with real-time information and data to help them make better clinical and surgical decisions. This includes alerts for potential drug interactions or allergies and recommendations for appropriate treatments.

viii. Cloud Storage: Cloud storage enables healthcare providers to store and access large amounts of patient data securely and remotely, allowing for efficient data management and sharing.

ix. Edge-enabled Healthcare Infrastructure: For large-scale and rural healthcare deployments, reliance solely on centralized cloud infrastructure may create latency, bandwidth, and privacy challenges. Edge computing enables localized data processing, real-time diagnostics, and reduced dependency on continuous high-bandwidth connectivity. Training AI models closer to data sources strengthens privacy, reduces operational cost, and enhances responsiveness in time-sensitive healthcare applications such as tele-ICU, connected ambulances, and emergency

services. An edge-first architecture can significantly improve scalability and resilience of digital health systems, particularly in geographically remote and connectivity-constrained environments.

x. Cybersecurity: Robust cybersecurity measures including encryption, access control, structured risk management frameworks, and Zero Trust principles are essential to protect electronic health information in digitally connected healthcare ecosystems.

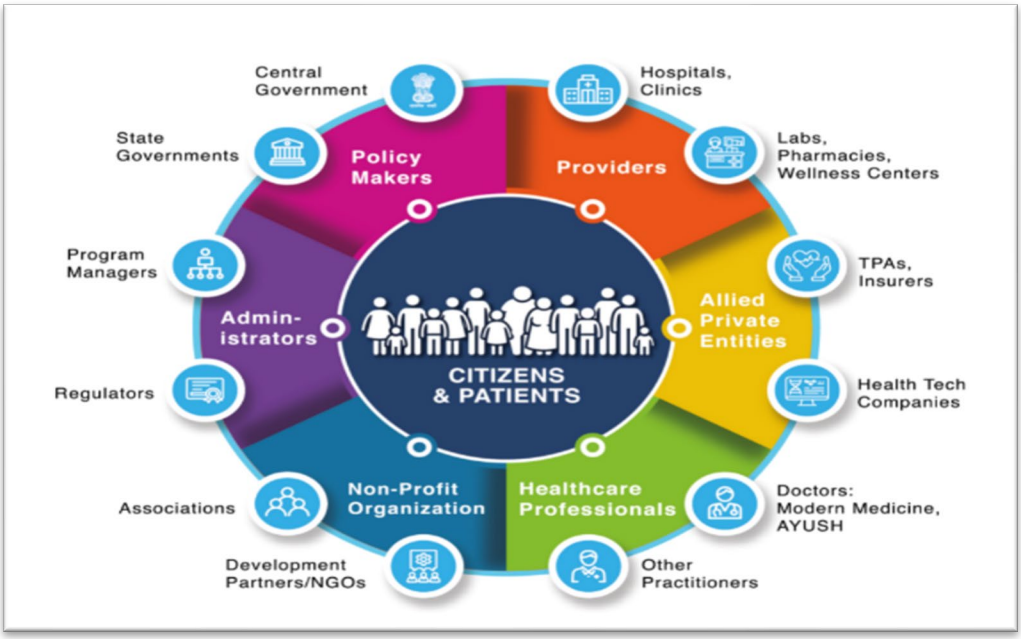
xi. Competent Digital Workforce: A competent and trained digital workforce is essential to drive digital transformation in healthcare sector.

5.3.3.1. Government-Led Digital Health Initiatives

The National Digital Health Mission has launched Ayushman Bharat Digital Mission (ABDM), which provides:

i. Ayushman Bharat Health Account (ABHA) Number, which is a 14-digit UHID
ii. ABHA app for maintaining Personal Health Records (PHR)
iii. Unified Health Interface (UHI) network to interconnect participating Health Service Providers (HSPs) and end-user applications

FIGURE 5: DIGITAL HEALTH ECOSYSTEM UNDER AYUSHMAN BHARAT DIGITAL MISSION (ABDM)



The initiative represents significant effort to create a comprehensive health information exchange network in India. As the program evolves and matures, it will greatly improve coordination and quality of care for patients throughout the country.

Centre for Development of Advanced Computing (CDAC)'s eSanjeevani is a web-based, comprehensive telemedicine solution. It extends the reach of specialized healthcare services to the masses, including those in rural and isolated communities. eSanjeevani can also be used

to provide medical education to interns and people across various Common Service Centres (CSCs).

National Informatics Centre (NIC)'s e-Hospital application is being offered to the Government Hospitals across the country through Software as a Service (SaaS) model. The modules of e-Hospital application which are currently available on the cloud include patient registration (OPD & casualty), IPD (admission, discharge & transfer), billing, laboratory information system, Radiology Information System, Clinic, Dietary, Laundry, Store & Pharmacy and OT Management. It is currently being used by over 268 hospitals across the country.

5.3.3.2. Infrastructure-Specific Recommendations

i. Every patient should be registered and provided a Universal Health Identification (UHID). Ayushman Bharat Health Account (ABHA) number can be used as a 14-digit UHID. It should be mandatory for all health service providers to use the same UHID for maintaining patient records.
ii. There is a need to mandate all health Provider to connect to Ayushman Bharat Digital Mission (ABDM) network.
iii. There is a need to develop regulatory compliance frameworks equivalent to HIPAA, which every digital healthcare system must comply with. Additionally, appropriate legal provisions should be in place to penalize non-compliance.

5.3.3.3. Data Management Challenges

Effective digital healthcare and AI adoption are constrained by challenges related to medical data quality, fragmentation, and governance. Large volumes of healthcare data are generated across clinical systems, imaging platforms, medical devices, and administrative workflows; however, much of this data remains unstructured, inconsistently documented, and siloed due to legacy practices. Limited availability of clean, structured, and annotated datasets restricts advanced analytics and AI-driven applications. Strengthening data governance, metadata management, and structured data capture mechanisms is essential for scalable AI adoption and evidence-based healthcare planning. Structured and computable healthcare datasets form the foundation for reliable AI models, predictive analytics, and population health management systems.

A key global focus is on strengthening health systems through resilience and resource efficiency by leveraging data and digital tools, reinforcing the need for structured gap analysis and standardized digital frameworks in India.

These foundational infrastructure components collectively enable scalable and secure healthcare applications across vertical domains.

5.3.4. Immersive Technologies

5.3.4.1. Digital Twins

In digital twins, virtual models of physical objects and humans are created. These virtual models are based on data captured using various sensors in devices such as IoT devices. Digital twins are used across multiple domains to monitor, analyse, and optimise workflows. They help with predictive analytics and simulations by representing the real world in a digital environment. In a digital twin environment, there is always a physical entity that refers to or is linked with a virtual entity.

In telehealth, digital twins are considered an immersive technology for next-level patient care, optimising healthcare services, and advancing medical research. Potential challenges in digital twin technology include data privacy and the complexity of the human body.

There may be multiple use cases across different domains. When considering the healthcare domain, the following use cases may be considered:

i. Digital twins can be created to represent patients by incorporating data from electronic health records (EHRs), medical imaging, genetic information, and other sources. These can help healthcare providers simulate disease progression, predict treatment outcomes, and personalize treatment plans.
ii. Surgeons can use digital twins to plan and simulate complex surgical procedures before operating on patients. By analyzing anatomical structures and simulating different surgical approaches, surgeons can optimize their techniques, reduce surgical risks, and improve patient outcomes.
iii. Digital twins can lead to revolutionary approaches in drug discovery and research. Chemical compound interactions may be simulated to assess the effectiveness and potential side effects of drugs during clinical trials. Patient-specific drugs can be developed using patient digital twins.

Overall, healthcare service delivery can be improved, leading to optimised remote patient care.

5.3.4.2. AI-enabled Clinical Trials and Cohort Selection

Clinical trials are a critical component of medical research, where the selection of an appropriate patient population is essential for evaluating the safety and efficacy of new drugs and therapies. Inefficient patient recruitment remains one of the most significant challenges in clinical research, contributing to increased costs, extended timelines, and trial failures. Phase III clinical trials, in particular, experience a high failure rate due to issues related to inadequate or incorrect patient recruitment, leading to wastage of time, resources, and investment.

AI- and digital twin–based approaches can significantly enhance clinical trial design and execution by enabling data-driven cohort identification and simulation. By leveraging historical clinical data, electronic health records, imaging data, and population health

datasets, AI models can assist in identifying suitable patient cohorts that best match trial eligibility criteria. Digital twins of patient populations can be created to simulate disease progression, treatment response, and trial outcomes, enabling researchers to optimize study design before actual enrollment.

Predictive AI models can further reduce redundancies in the patient recruitment process by forecasting enrollment risks, identifying underrepresented patient groups, and improving cohort composition. This approach supports more efficient recruitment strategies, improves statistical validity, and enhances the likelihood of trial success. The integration of AI-enabled digital twins in clinical trials can therefore accelerate research timelines, reduce costs, and improve the overall effectiveness of drug development and translational research.

5.3.4.3. Metaverse Aspects

The Metaverse is the three-dimensional (3D) Internet, or a shared virtual environment comprising a collection of virtual worlds accessed by individuals via the Internet. It has the potential to extend the physical world using augmented and virtual reality technologies, allowing users to seamlessly live, interact, socialize, learn, play games, and shop within a self-sustaining, persistent, and shared realm across real and simulated environments using avatars and holograms. The Metaverse is becoming increasingly relevant to daily life and is expected to impact society in the coming decades by enabling immersive experiences in both virtual and physical environments. Individuals enter the Metaverse through the following four technologies: virtual reality (VR), augmented reality (AR), mixed reality (MR), and extended reality (XR).

The COVID-19 pandemic increased interest in online healthcare delivery due to reduced social and business interactions, leading to the increased adoption of advanced technologies such as the Metaverse in the healthcare sector. Major healthcare companies and hospital chains are increasingly joining the virtual world of the Metaverse to improve patient care.

According to a Market Research Future report (ID: MRFR/ICT/9416-HCR | January 2023), the global healthcare Metaverse market is expected to reach USD 5.8 billion by 2030, expanding at a compound annual growth rate (CAGR) of 48.3% from 2024 to 2030, indicating that many patients have already joined or are considering joining this virtual space. Telemedicine and telepresence (allowing people to be together virtually), digital twinning (creating virtual models that accurately reflect physical objects), and blockchain (enabling a distributed internet) are key drivers of Metaverse adoption in the healthcare sector.

The global Metaverse market is projected to grow from USD 11.47 billion in 2023 to USD 107.49 billion by 2030, exhibiting a CAGR of 45.2% during the forecast period 2022–2030.

a. Healthcare Metaverse Use Cases (Rural Context)

Metaverse technologies can enhance healthcare delivery in rural and remote regions by enabling virtual specialist consultations, remote-assisted surgeries, and immersive diagnostic interactions. Integration with IoT-enabled devices can support virtual body scans and real-time vitals monitoring within a digital environment. Additionally, immersive platforms can facilitate medical education and clinical skill training through simulated environments, improving access to quality healthcare expertise across geographies.

b. The Opportunity for Healthcare and Wellbeing in the Metaverse

The Metaverse has the potential to significantly impact how people and tech interact, access, and receive medical care/healthcare and offers significant opportunities for emotional wellbeing / mental health, and physical health.

c. Mental Health and Emotional Wellbeing in Metaverse

The World Health Organization (WHO) defines Mental health as an integral component of health and wellbeing that supports our individual and collective abilities to make decisions, build relationships and shape our society. Mental health is critical to personal, social, community, and socio-economic development and is a fundamental human right.

According to the United Nations World Mental Health Report, over one billion people across the globe suffer from mental health disorders, and depression and anxiety are among the most prevalent. During the first year of the COVID-induced pandemic, anxiety and depression are estimated to have increased by 25% globally, as per the same WHO report.

India is no exception; in fact, India has one of the highest prevalence rates of mental illnesses globally. The National Mental Health Survey (2019) reported that approximately 14% of the adult population in India currently have or will experience some form of mental health condition. This translates to an estimated 56 million individuals dealing with depression and an additional 38 million individuals affected by anxiety disorders. The World Health Organization indicates that the economic impact of inadequate mental health in India is projected to exceed USD 1.03 trillion from 2012 to 2030.

d. Mental Health Challenges in the Indian Context

Mental health in India faces several challenges, reflecting a complex interplay of socio-cultural, economic, and systemic factors. These challenges have significant implications for individuals, families, communities and society overall. Some of the critical challenges for mental health in India include:

i. Stigma and discrimination are among the most significant challenges associated with mental illnesses. People with mental health issues often face social exclusion, leading to delayed or inadequate treatment seeking. This led to people being private or silent about their mental health conditions and continuing suffering without seeking help or discussing it with their family and friends.
ii. Limited Mental Health Infrastructure leads to a severe shortage of mental health professionals, psychiatric hospitals, and counselling centers. According to the World Health Organization (WHO), India has only one psychiatrist for every 343,000 people, well below the global average of 3 Psychiatrists per 100,000.
iii. Lack of awareness and education about mental health in India, many individuals fail to recognize the signs of mental illnesses or misunderstand them as character flaws. This lack of awareness hampers early intervention and effective treatment.
iv. Rapid urbanisation, high population density, and modern lifestyle also contribute to stress, anxiety, and other mental health issues across the population.
v. Inadequate government funding causes lack of resources and leads to limited access to affordable and quality care for most of the population.

e. Mental Health Assessment in Metaverse

The Metaverse, by providing innovative and immersive tools for understanding individuals' emotional wellbeing, has the potential to revolutionize mental health assessment. By leveraging virtual reality and advanced technologies, mental health professionals can conduct more accurate, personalized, and ecologically valid assessments.

i. Use Case 1 - Metaverse can offer Immersive Environments for Assessment: Using Metaverse's virtual reality (VR) capabilities, real-life situations, such as social interactions, public speaking, or facing specific fears, can be simulated and the mental health professionals can gain valuable insights into individuals emotional and psychological state by observing their real-time behavioural responses and reactions within these environments and make accurate assessments.
ii. Use Case 2 - Remote Assessments and Telepsychiatry: The Metaverse's ability to connect people across geographical distances allows for remote mental health assessments and telepsychiatry services for individuals in remote or underserved areas without the need for physical travel, improving accessibility to mental healthcare services.
iii. Use Case 3 - Monitoring Long-term Progress: The Metaverse can facilitate long-term monitoring of mental health conditions by tracking users' interactions, behaviors, and responses over time. This continuous data collection enables mental health professionals to detect changes in a person's emotional wellbeing and provide timely interventions when necessary.
iv. Use Case 4 - Incorporating Biofeedback and Physiological Responses: By integrating biofeedback and physiological monitoring devices, such as heart rate monitors and EEG headsets with Metaverse, mental health professionals during virtual assessment can capture real-time physiological responses and can gain valuable insights into an individual's emotional arousal and stress levels.
v. Use Case 5 - Multimodal Data Analysis: The Metaverse generates a vast amount of multimodal data, including audio, video, and behavioural data, during virtual assessments. Using advanced data analytics and artificial intelligence (AI) techniques, extract patterns and insights that may not be readily apparent through traditional assessments.

f. Virtual Therapeutic Interventions in Metaverse

Virtual therapeutic interventions in the Metaverse have the potential to complement and offer innovative and effective ways to address various mental health challenges by leveraging the immersive and interactive nature of virtual reality and augmented reality.

i. Use Case 1 - Cognitive Behavioural Therapy (CBT) Interventions: The Metaverse can help in CBT interventions by providing virtual scenarios for challenging negative thought patterns and cognitive distortions. Mental health professionals can guide patients through these scenarios to promote cognitive restructuring and more adaptive thinking.
ii. Use Case 2 - Cognitive therapy for Autism patients: Studies performed at the University of Texas and Northwestern University's Psychiatry Department on patients with autism receiving cognitive therapy using VR programs that use avatars

to simulate job interviews and meetings have proven to be successful in improving life skills, as well as overall improvement in concentration, cognition, and memory.

iii. Use Case 3 - Phobia and Exposure Therapy: Evidence reveals that virtual reality (VR) effectively treats phobias. By integrating exposure therapy into the Metaverse, the therapy becomes more effective and accessible. Metaverse can offer a safe, economical, practical, and reliable exposure therapy platform to treat people with a phobia, including a phobia of Water, Height, Flying, Public Speaking, thunderstorms, etc. VR medical center having VR equipment were established in the USA to treat phobic patients in the most suitable, affordable, and convenient way. The center treats several phobias, including flying, fear of driving, public speaking, and thunderstorm phobia.

iv. Use Case 4 - Social Behaviour/Skills Training: Virtual environments in the Metaverse can be a safe space for individuals to practice and improve their social skills. This is particularly beneficial for those with social anxiety or communication difficulties.

g. Relaxation and Stress Reduction

Virtual environments in Metaverse can be designed to promote relaxation and stress reduction.

i. Use case 1 - Guided meditation sessions and tranquil nature scenes: Virtual reality can facilitate guided meditation and mindfulness sessions. Users can use VR headsets to participate in virtual meditation sessions led by experienced instructors in remote locations. Guided practices help individuals focus on the present moment, reduce rumination, and cultivate inner peace.

ii. Use case 2 - Mindful Movement and Yoga: Virtual reality can facilitate mindful movement practices like yoga. Users can participate in virtual yoga classes led by instructors guiding them through various postures and sequences that promote relaxation and body awareness.

h. The Challenges in Adoption of Immersive Healthcare Technologies

Overall, healthcare applications in the Metaverse, within the context of telemedicine, telepresence, and digital twinning, can provide new opportunities for healthcare delivery. However, these opportunities also introduce several challenges, including:

i. Privacy and security: The Metaverse can raise concerns about the privacy and security of personal health data, as well as the potential for manipulation of users' experiences and the spread of misinformation.

ii. Ethical considerations: The Metaverse raises ethical concerns related to data ownership, virtual identity, and the potential to manipulate patients' experiences

iii. Limited accessibility: Not all patients have access to the technology required to use the Metaverse, and some may find it challenging due to physical or cognitive limitations.

iv. Lack of standardization: The Metaverse is a new and rapidly evolving field, and there is limited standardization in technology and design. This can make it difficult for healthcare providers to design and implement effective virtual environments and

interfaces. Addressing these challenges will require careful consideration and further research.

v. Acceptance and adaptation to new technology: Healthcare providers and patients may require training and ongoing support to use immersive technologies effectively.
vi. User trust: Building trust in virtual environments can be challenging, as patients may be skeptical of the information and interactions encountered in the Metaverse.
vii. User experience: Ensuring a positive user experience in the Metaverse can be difficult, as users may find it challenging to navigate virtual spaces or may experience discomfort or nausea while using VR/AR technologies.

Artificial Intelligence complements technologies such as 5G, cloud computing, and immersive platforms by enabling data analysis and supporting better clinical and operational decisions in healthcare.

5.3.5. Telehealth Best Practices and Insights

Telehealth should focus on practices which help patients ensure the delivery of healthcare service on time with quality and maintain the safety & privacy of patients. C-DAC follows and recommends end users of its Mercury™ Telemedicine solution during its usage in telehealth improving access to services and increasing outcomes:

i. Secured Telehealth Platform: It is always recommended to follow security measures while developing a telehealth platform, considering vulnerabilities in the production, deployment, and usage environments. It is highly recommended to apply high-level encryption to patient data during storage and transfer. The Mercury™ solution uses the latest encryption and hashing algorithms for storage and transfer of patient records. It is also recommended that the platform be audited by a certified agency for security purposes.
ii. Train end user for Telehealth Platform: The C-DAC's Mercury™ team always provide training on the platform to end users by providing them with the knowledge and skills they require to operate and use their regular workflow effectively to accomplish their activities related to Telehealth.
iii. Encourage end users to use: Provide technical support to users to help them navigate telehealth platforms and troubleshoot any issues they may encounter during telehealth consultations.
iv. Patient Consent: Provide patients with clear information about telehealth services, including how they work, potential risks, and benefits. Obtain informed consent from patients before delivering telehealth services. Ensuring patients feel comfortable and engaged during telehealth consultations.
v. Following Clinical Protocols: Develop clinical protocols and guidelines for telehealth consultations to ensure consistency and quality of care delivery. Consider adapting existing clinical guidelines for in-person care to the telehealth context.
vi. Compliance with government regulations: Ensure compliance with all relevant healthcare regulations, and policies of the government.

vii. Evaluation based on feedback and upgrades: Regularly evaluate the effectiveness of telehealth services and identify areas for improvement. User feedback helps to enhance the quality of care.
viii. Support for Patients: Maintaining a comfortable environment for communication ensures patient engagement during telehealth consultations. This improves the patient-healthcare provider relationship, which is essential for building patient confidence.

5.4. Advanced Data-Driven Intelligence in Healthcare

Artificial Intelligence operates as a cross-cutting intelligence layer across the healthcare ecosystem, enabling enhanced analytics, decision support, automation, and system optimisation. It is positioned as an enabling tool that augments human-led healthcare systems by enhancing diagnostics, optimizing workflows, and supporting preventive care, while remaining aligned with clinical oversight and regulatory frameworks.

AI systems deployed in healthcare must also support regional language processing, including voice recognition and speech-based interaction, to ensure inclusive access across diverse linguistic populations in India.

AI is increasingly adopted across the healthcare value chain to suport preventive care, disease diagnosis and prediction, treatment planning, care delivery, and administrative operations. AI-enabled systems support improved accessibility to healthcare services, particularly in remote and underserved regions, by enabling point-of-care diagnostics, teleconsultation, and automated clinical decision support. These systems improve efficiency through faster diagnosis, optimized workflows, and cost- and time-efficient care delivery.

Despite these benefits, the adoption of AI in healthcare presents several challenges and risks. These include the bias in AI models arising from incomplete or non-representative datasets, concerns related to data privacy and cybersecurity, and risks associated with the misuse or unauthorized access to sensitive health information. In addition, increased automation may have implications for employment patterns and skill requirements within the healthcare workforce, necessitating reskilling and capacity-building initiatives. Addressing these risks is essential to ensure responsible and trustworthy deployment of AI in healthcare systems.

To maximize the opportunities offered by AI while mitigating associated risks, the World Health Organization (WHO) has proposed six guiding principles for the ethical and responsible use of AI in healthcare:

i. Protecting human autonomy, ensuring that AI supports, rather than replaces, human decision-making.
ii. Promoting human well-being, safety, and the public interest.
iii. Ensuring transparency, explainability, and intelligibility of AI systems.
iv. Fostering responsibility and accountability among AI developers and deployers.
v. Ensuring inclusiveness and equity, so that AI benefits are accessible across diverse populations.
vi. Promoting sustainable and responsive AI, aligned with long-term societal and healthcare goals.

Adherence to these principles can help ensure that AI serves as a trusted, equitable, and effective enabler within the digital healthcare ecosystem.

5.4.1. Components of AI Implementations in Healthcare

i. Descriptive: Analysis and summarization of historical data.
ii. Diagnostic: Root-causes analysis of trends.
iii. Predictive: Forecasting outcomes based on historical data and trends.
iv. Prescriptive: Decision recommendation using trained models.
v. Cognitive: semi-autonomous monitoring and decision making.

5.4.2. AI-driven Data Analytics for Hospital Operations

Artificial Intelligence–driven data analytics plays a significant role in enhancing hospital management, operational efficiency, and patient care quality. By analysing historical and real-time data, AI systems enable predictive, prescriptive, and operational decision support across multiple hospital functions.

Key applications include:

i. Demand Forecasting: Predicting outpatient visits, emergency admissions, and bed occupancy trends to optimize resource allocation.

ii. Staff Optimization: Intelligent scheduling of doctors, nurses, and support staff based on patient load and peak demand periods.

iii. No-Show Prediction: Identifying patients likely to miss appointments and enabling proactive reminders or rescheduling strategies.

iv. Supply Chain Optimization: Forecasting inventory requirements for medicines, consumables, and critical equipment to reduce wastage and shortages.

v. Fraud Detection: Identifying anomalies in billing patterns, insurance claims, and financial transactions.

vi. Reduction of Medical Errors: Analyzing clinical data to flag potential drug interactions, incorrect dosages, and treatment inconsistencies.

AI-driven analytics strengthens data-informed decision-making and contributes to improved operational resilience, cost efficiency, and patient safety within healthcare institutions.

5.4.3. Blockchain for Health Information Exchange

Blockchain technology offers a secure and tamper-resistant mechanism for health information exchange across distributed healthcare systems. Using decentralized ledger frameworks, blockchain can enhance data integrity, enable transparent audit trails, strengthen patient identity management, and reduce intermediaries in health record transactions. When integrated with existing digital health platforms, blockchain can support trusted, interoperable, and secure exchange of electronic health records.

6. Regulatory aspects – ICT and non-ICT

The Telemedicine Practice Guidelines (TPG), introduced by the Government of India in March 2020, serve the purpose of standardizing telemedicine practices. These guidelines align with the definition presented by the World Health Organization (WHO), which characterizes telemedicine as "the use of information and communication technologies by healthcare professionals to deliver services when distance is a critical factor."

Through the integration of information and communication technology (ICT) in the healthcare sector, diverse tools and services are harnessed to prevent, mitigate, diagnose, treat, and monitor various health conditions. The incorporation of genetic insights and digital innovations for early disease identification and prompt intervention embodies the essence of digital health. Oversight of this sector falls under the purview of the Ministry of Health and Family Welfare (MoHFW) within the Government of India.

Several noteworthy emerging technologies within India's digital healthcare framework include wearable digital diagnostic instruments; software and hardware for remote monitoring and tracing; telemedicine solutions; mobile health applications; machine learning integration; advancements in medical imaging; utilization of big data; implementation of the Internet of Medical Things (IoMT); facilitation of robot-assisted surgery; devices for self-monitoring healthcare metrics; maintenance of electronic health records (EHRs); utilization of targeted advertising; exploration of personal genomics; personalized or precision medicine approaches; biomarker-based tools; e-pharmacy platforms; cloud computing technologies; incorporation of artificial intelligence (AI); and the adoption of augmented and virtual reality solutions.

Ensuring the security of health-related information exchanged between patients and healthcare providers, along with associated recommendations and outcomes, is of paramount importance. To address this need, provisions within the Information Technology Act, 2000, along with its amendments, and the Digital Personal Data Protection Bill, 2023, are designed to apply across all scenarios.

As the array of digital and innovative healthcare technologies expands, concerns regarding patient privacy and data security also increase. Despite the majority of healthcare providers adhering to India's existing data privacy laws for data collection, storage, and usage, significant apprehensions persist regarding potential data misuse and privacy obligations.

The absence of adequate education and training for personnel responsible for managing patient data within digital health platforms further exacerbates the situation.

The Personal Data Protection Bill, introduced in the Lok Sabha on December 11, 2019, introduced the concept of a Data Protection Authority aimed at safeguarding individuals' personal data. However, the withdrawal of the bill from Parliament on August 4, 2022, signaled a shift in approach.

The government proposed introducing a suite of new laws focusing on social media, digital technology, telecommunications, and privacy, rather than a single comprehensive law. Accordingly, specialized statutes addressing distinct aspects of the digital technology sector

were envisaged, and a new act providing a comprehensive legal framework has been introduced in the form of the Digital Personal Data Protection Bill (DPDPB), 2023.

Additionally, the proposed Digital Information Security in Healthcare Act (DISHA) aims to establish national and state health authorities to prevent the unauthorized sharing of health-related data with third parties. To further safeguard digital health data, the Ministry of Health and Family Welfare (MoHFW) has formulated a National Digital Health Mission–related Health Data Management Policy.

IoMT deployments introduce heightened privacy and compliance obligations due to continuous collection and transmission of sensitive health data. In India, such systems must align with the Digital Personal Data Protection (DPDP) Act, 2023 and the proposed Digital Information Security in Healthcare Act (DISHA), which emphasize consent management, data minimization, secure storage, and controlled data sharing.

As IoMT ecosystems expand, regulatory oversight similar in spirit to HIPAA-like frameworks becomes increasingly relevant to ensure lawful processing and protection of patient health information.

6.1. Policy and Regulatory Gaps for Artificial Intelligence in Healthcare

At present, the use of Artificial Intelligence (AI) in healthcare in India is not governed by a dedicated, AI-specific regulatory framework. AI-enabled healthcare applications are primarily regulated under existing information technology and data protection laws, including the Information Technology Act and the Digital Personal Data Protection framework.

While these laws provide a baseline for data security, privacy, and accountability, they do not explicitly address AI-specific concerns such as algorithmic transparency, bias mitigation, explainability, or clinical responsibility in AI-assisted decision-making. As AI adoption in healthcare continues to grow, there is a need to evolve sector-specific guidance and regulatory frameworks to ensure safe, ethical, and responsible deployment of AI in healthcare systems.

6.2. Regulatory Models and Schemes in India

In India, the domain of digital health operates under a set of laws, guidelines, and standards. While each digital health tool or business model possesses individual governance mechanisms, several regulations apply universally to digital health technologies.

The legal landscape encompasses key legislations such as the Information Technology Act (IT Act), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), the Information Technology (Intermediary Guidelines) Rules, 2011 (Intermediary Guidelines), and the Digital Personal Data Protection Bill (DPDPB), 2023. Together, the IT Act, SPDI Rules, Intermediary Guidelines, and DPDPB constitute India’s overarching data protection framework.

The enhanced security provisions outlined in the IT Act have paved the way for secure online transactions and the seamless transfer of electronic data. The IT Act encompasses a wide

spectrum of online activities, including the validation of digital signatures and the legal recognition of electronic records.

Furthermore, the IT Act addresses diverse forms of cybercrime, ranging from hacking to denial-of-service attacks. The existing legal system in India that aims to protect electronic health (e-health) information primarily relies on the IT Act and the SPDI Rules. These rules provide a certain level of security concerning the collection, sharing, and transfer of sensitive personal data, including medical records and health histories.

Nevertheless, as technology advances rapidly, this legal framework has faced challenges in keeping pace, leaving certain crucial matters unresolved. As a result, medical establishments and practitioners in India are progressively embracing Electronic Medical Records (EMRs) and Electronic Health Records (EHRs).

As per the regulations outlined in the Clinical Establishments (Registration and Regulation) Act, 2010, every medical facility is required to maintain an Electronic Medical Record (EMR) for each patient, along with relevant registration documentation.

The Ministry of Health and Family Welfare (MoHFW) introduced the Electronic Health Record (EHR) Standards in 2013, which were later revised and released in December 2016. These standards provide an internationally aligned framework that healthcare providers can utilize to create and manage EHRs.

The MoHFW is actively implementing a range of ongoing digital health initiatives. These include, but are not limited to, Reproductive Child Healthcare (RCH), Integrated Disease Surveillance Programme (IDSP), Integrated Health Information System (IHIS), e-Hospital, e-Sushrut, Electronic Vaccine Intelligence Network (eVIN), Central Government Health Scheme (CGHS), Integrated Health Information Platform (IHIP), National Health Portal (NHP), National Identification Number (NIN), and the Online Registration System.

These initiatives are deeply embedded within the healthcare sector and continuously generate substantial data that holds potential for public health improvement. As health is a state subject, the National Health Mission (NHM) provides financial assistance to states for integrated services such as telemedicine, teleradiology, tele-oncology, tele-ophthalmology, and hospital information systems.

Enacted in 2000, the Designs Act primarily offers protection to consumer-oriented items. This legal framework focuses on characteristics related to shape, configuration, pattern, ornamentation, or composition of lines and colors applied to a tangible object, referred to as an “article.”

Within the digital health domain, two critical elements requiring design protection include visual user interfaces (UIs) and device configurations. The Designs Act extends protection to UIs through provisions specified in Article 14-04 of the Design Rules, 2001, which addresses “Screen Displays and Icons.”

Furthermore, the Central Drugs Standard Control Organisation (CDSCO) has published an initial list of risk-based classifications for medical devices under the New Definition Notification. This list categorizes medical devices into 24 categories, aligned with

internationally accepted classification norms, and also specifies separate classifications for standalone medical device software.

The CDSCO serves as the central regulatory authority responsible for enforcing the Drugs and Cosmetics Act, 1940, along with its associated rules. Regulation of medical practice was earlier overseen by the Medical Council of India, while intellectual property protection falls under the Office of the Controller General of Patents, Designs, and Trademarks (CGPDTM), and copyright-related matters are administered by the Copyright Office.

Both organizations function under the Department for Promotion of Industry and Internal Trade (DPIIT). In collaboration with the National Digital Health Blueprint (NDHB) and MoHFW, the Indian Council of Medical Research (ICMR) has played a significant role in advancing healthcare research initiatives.

The primary legal and regulatory framework is predominantly shaped by the following key legislations:

i. The Information Technology Act, including the SPDI Rules and the Information Technology Rules, 2011
ii. The New Telecom Policy, 1999, defining requirements for Other Service Providers
iii. The Drugs and Cosmetics Act, 1940, along with the Drugs and Cosmetics Rules, 1945
iv. The Indian Medical Council Act, 1956, and the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002
v. The Drugs and Magic Remedies Act, 1954, and the Drugs and Magic Remedies Rules, 1955
vi. The Commercial Communication Customer Preference Regulations, 2010, and the Unsolicited Commercial Communications Regulations, 2007
vii. The Clinical Establishments Act, 2010
viii. The Digital Personal Data Protection Bill, 2023

6.2.1. Issues relating to use of personal data

Ensuring data privacy holds paramount importance when it comes to the utilization and implementation of personal data. In the year 2013, India initiated its inaugural Electronic Health Record (EHR) Standards. These standards were chosen based on their suitability for the Indian context, drawn from the most effective internationally recognized EHR standards that had been previously put into practice.

This effort culminated in the refinement of the 2016 EHR Standards document, which was then incorporated into the national IT systems to be adopted by healthcare institutions and providers.

To facilitate its adoption, MoHFW took proactive measures. This included making standards like the Systematized Nomenclature of Medicine Clinical Terminology (SNOMED CT) available for free use within India. Furthermore, the MoHFW established an interim National Release

Centre to oversee the management of this clinical terminology standard, which has been gaining global recognition within healthcare IT stakeholder communities.

In addition to these initiatives, the MoHFW has proposed the introduction of a new bill, known as DISHA, aimed at regulating data security within the healthcare sector. The primary objective of this Act is to safeguard the privacy, confidentiality, security, and standardization of Electronic Health Records (EHRs).

The MoHFW's plan includes the establishment of DISHA to actively promote and adopt e-health standards, enforce robust privacy and security measures for electronic health data, and oversee the organized storage and exchange of EHRs. These regulations delineate the extent to which information can be utilized, subject to consent from both beneficiaries and service providers.

They also outline the criteria for categorizing "sensitive health-related information" and "sensitive personal information."

For example, when a patient goes to a doctor for a check-up and the doctor accesses the patient's past medical history and records the current diagnostic findings in an EHR, the DISHA ensures the security of this information as it traverses through the healthcare system.

DISHA lays out three primary goals for safeguarding data: setting up a national and state digital health authority, enforcing privacy and security protocols for electronic health data, and overseeing the storage and exchange of electronic health information.

Furthermore, the proposal advocates for the establishment of national and state electronic health authorities (NeHA and SeHA) with the aim of providing comprehensive data protection and healthcare management to Indian citizens. These authorities also ensure and oversee data portability.

Machine learning plays pivotal roles within the domain of digital health, encompassing a range of functions such as streamlining diverse methods and processes to enhance efficiency and cost-effectiveness. It aids in disease identification and early detection, contributes to drug development and manufacturing, analyses behavioural changes using machine learning insights, ensures the safekeeping and security of medical records, predicts disease outbreaks, and supports clinical trials, data gathering, and data analysis.

Machine learning plays pivotal roles within the domain of digital health, encompassing a range of functions such as streamlining diverse methods and processes to enhance efficiency and cost-effectiveness. It aids in disease identification and early detection, contributes to drug development and manufacturing, analyses behavioural changes using machine learning insights, ensures the safekeeping and security of medical records, predicts disease outbreaks, and supports clinical trials, data gathering, and data analysis.

Given the current lack of dedicated regulations for artificial intelligence (AI), cloud computing, and machine learning in India, initiatives involving these technologies must comply with existing IT laws and regulations. Employing confidentiality agreements between data owners and licensees, along with clearly defined data usage strategies, can help mitigate risks.

Liabilities arising from adverse outcomes may be civil or criminal in nature and vary depending on whether they involve medical practitioners or service providers such as institutions and internet service providers. In addition to civil remedies, recourse under the Consumer Protection Act may be pursued.

In cases of medical negligence, patients may file complaints with the ethical committee of the Medical Council of India. The Indian Penal Code also addresses criminal accountability, which remains relevant in the context of digital health solutions.

A persistent challenge in digital health is the high cost associated with establishing and maintaining health IT infrastructure, alongside the need for secure data storage while ensuring confidentiality and privacy.

Equally important is the evaluation of data security and privacy across all stages of data processing. Data localization and responsible data usage are therefore of critical importance.

In recent years, India's digital healthcare sector has increasingly focused on innovation and technological advancement. In the Union Budget 2022, the Government of India announced plans to introduce an open platform for the National Digital Health Ecosystem, including digital healthcare provider registries and access to health facilities.

The government also announced the launch of the National Tele-Mental Health Programme, aimed at providing high-quality mental health counselling and care services across all age groups, with plans to establish 23 tele-mental health centres nationwide.

Looking ahead, approximately 80% of healthcare systems are expected to increase investments in digital health tools over the next five years. Indian innovators are actively developing advanced health-tech products and solutions, with implementation being driven through the Ayushman Bharat Digital Mission (ABDM).

The rollout of ABDM further strengthens India's efforts toward healthcare digitization.

Another significant initiative introduced in 2022 is the Unified Health Interface (UHI), a digital platform designed to connect healthcare providers and patients for services such as appointment bookings and consultations.

As the healthcare sector continues to evolve rapidly, there is a strong likelihood that a comprehensive and unified digital health law will be enacted in the near future.

7. Tele-ICU System

Tele-ICU systems aim to achieve mechanisms for optimum utilization of critical care experts across ICUs. Tele-ICU can be categorized into multiple domains and specialties. A typical system adheres to various medical standards, security standards, and high-speed network facilities. Periodic reporting of clinical and administrative data is provided to analyze and improve the overall treatment environment.

ICU medical devices capture clinical parameters of patients, based on which a remote ICU specialist provides diagnosis and treatment. Any change in parameters resulting in a decline in a patient's health should be notified immediately. Transfer of clinical parameters to the command centre or specialist, or the generation of alert notifications, should be performed with low latency. As these are time-critical services, underlying networks should provide low latency, such as 5G networks. Software used in Tele-ICU systems and medical devices should be optimized to effectively utilize such networks.

Medical devices available in the market often generate data in non-standard or proprietary formats, making integration a tedious task. ICU devices should generate data in relevant standard formats, and generic APIs should be provided to enable integration and data capture into other healthcare systems.

Critical cases require immediate medical action whenever there is a change in a patient's medical condition. In such situations, notifications should be sent to treating or on-duty medical professionals. Alerts or messages from medical professionals should also be communicated to the command centre to enable preparedness for such situations.

TeleICU ecosystem includes following key players:
Infrastructure and Software

i. ICU devices
ii. Centralized Servers
iii. Command Centre
iv. Monitoring station display
v. eICU Management Software
vi. High Speed Internet Connectivity
vii. Device Interfacing Software
viii. Other IT equipment

Manpower

i. Intensivists
ii. Nursing Staff
iii. Command center Operators
iv. IT Admin

7.1. Multi-Human Federated Telerobotic Session

A semi-autonomous collaborative telerobotic framework can further enhance Tele-ICU capabilities by enabling multiple medical experts to participate in a coordinated remote intervention session. In a multi-human federated model, a lead specialist may control or supervise a robotic system, while additional experts provide real-time guidance, analytics support, or decision validation through a shared digital interface.

Such systems allow distributed intensivists and domain specialists to collaboratively manage complex critical care scenarios with shared situational awareness. Semi-autonomous features, supported by AI-driven assistance and high-speed low-latency networks, can improve procedural precision, reduce response time, and extend expert reach to remote or resource-constrained facilities.

7.2. Tele-Education using AR/VR Platforms

Nowadays, healthcare services utilize the benefits of information technology. Medical education is also adopting the latest technologies to enable better healthcare education delivery. Rapidly evolving technologies such as Augmented Reality (AR) and Virtual Reality (VR) are well equipped to enhance user experiences. It is the need of the hour to incorporate such technologies into medical education.

The use of AR and VR technologies provides a more personalized user experience to medical students and offers an edge over traditional methods of education. With AR and VR tools, education and training programs can be conducted to enhance learning and improve clinical procedural experiences.

AR technology enables the display of overlaid objects combined with real-world elements on outputs such as TVs, mobile devices, projectors, and heads-up displays (HUDs). These overlaid objects may include textual data, media, images, etc., and are linked or tagged to real-world elements. In contrast, VR technology is completely immersive, utilizing head-mounted devices (HMDs) and body-tracking sensors. In this technology, VR content is used to display virtual information and enable interactive operations.

AR/VR technology is also useful in research and in visualizing experiments related to medical procedures and simulations.

With the help of AR and VR technology, medical professionals can learn and experience effective monitoring and analysis of patient health conditions, even in real time, and make informed decisions for better treatment outcomes.

AR/VR technology requires high bandwidth and low latency to ensure smooth content delivery. Hence, the underlying network must provide sufficient bandwidth and minimal latency.

Content development for tele-education remains a key challenge in this domain. The high degree of complexity and time required to develop and deliver such content creates barriers

to wider adoption of AR/VR technologies. To deliver such content to large numbers of users, a centralized platform can be established for content distribution through a centralized server.

Key challenges in AR/VR technology include simulator sickness, high-cost setups, limited availability of high-bandwidth networks, and tightly coupled hardware and software components.

One notable use case of AR/VR is the Virtual ICU. Existing infrastructure in ICUs is complex and involves tiered systems of fixed audio-visual communication, access to Electronic Medical Records (EMRs), telemetry, imaging systems for data retrieval and documentation, as well as risk stratification and decision-support systems.

FIGURE 6:FACILITIES THAT CAN BE VISUALIZED AND MONITORED THROUGH AR/VR-CONNECTED SYSTEMS INCLUDE MECHANICAL VENTILATORS, CONTINUOUS VENO-VENOUS HEMOFILTRATION (CVVH), EXTRACORPOREAL MEMBRANE OXYGENATION (ECMO), PATIENT ELECTRONIC RECORDS, HEMODYNAMIC MONITORS, DEFIBRILLATORS, AND INFUSION PUMPS.

8. Medical Standards for Healthcare Systems

Multiple standards need to be adhered to by healthcare solutions, including medical standards, security standards, and communication standards, for scenarios such as data exchange, data encryption, data capture standards, data storage, identification and demographics, medical imaging, and audit trails and logging.

Medical standards recommended to be followed by healthcare solutions include:

i. ISO/TS 22220:2011 and MDDS for identification and demographics
ii. UIDAI Aadhaar or government-issued photo identity card number for patient identification
iii. ISO 18308:2011 and ISO/HL7 10781:2015 for system and functional requirements, respectively
iv. SNOMED CT for terminology
v. LOINC and ICD for coding systems
vi. DICOM for medical imaging
vii. ISO/TS 14441:2013 for data security
viii. SHA-256 or higher, HTTPS, SSL v3.0, and TLS v1.2 for data encryption
ix. ISO 27789:2013 for audit trails
x. Pharmacy Practice Regulations, 2015, Notification No. 14-148/2012-PCI, as specified by the Pharmacy Council of India, for e-prescriptions
xi. FHIR, HL7 standards, CCD, ISO 13606-5:2010, and DICOM for data exchange
xii. JPEG, ISO/IEC 14496 (Audio-Visual Objects), and ISO 19005-2 for scanned or captured records

Implementation of medical standards enables interoperability within healthcare systems. Interoperability allows one healthcare system to exchange records with another healthcare system.

These challenges further emphasize the importance of adopting standardized data formats, coding systems, and interoperability frameworks as outlined in the section 3.2.3.

The Ayushman Bharat Digital Mission (ABDM) has been developed to provide an integrated digital health infrastructure for the country. This platform promotes healthcare system integration by bridging gaps between various providers within the healthcare ecosystem. The ABDM sandbox can be used to test integration and validation. The Ayushman Bharat Health Account (ABHA) number is used to uniquely identify individuals within the ABDM ecosystem. Systems can be integrated, and data exchange can be enabled using FHIR profiles.

The Ayushman Bharat Health Account (ABHA) identifier (ID) is a unique ID issued to individuals enrolled under the Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB-PMJAY) scheme in India. The ABHA ID facilitates the implementation of the Ayushman Bharat scheme by enabling eligible individuals to receive healthcare services under the health insurance coverage.

The benefits of having an ABHA ID include:

i. The AB-PMJAY scheme provides health insurance coverage of up to ₹5 lakh per family per year, offering protection against medical expenses.

ii. Beneficiaries can avail cashless treatment at empanelled hospitals and healthcare centres across India.

iii. Access to a wide range of healthcare services, including hospitalisation, surgery, and diagnostics, is provided under the scheme.

iv. Beneficiaries are allowed to receive treatment anywhere in India, supporting portability across states.

v. Coverage includes pre-existing medical conditions, unlike many private insurance schemes.

vi. The ABHA ID can serve as a repository of digital health records, enabling easier tracking of medical history, treatments, and prescriptions.

vii. By improving access to affordable healthcare, the scheme contributes to an improved quality of life for beneficiaries.

For generation of an ABHA ID, the following steps are followed:

i. Visit the AB-PMJAY website.

ii. Locate and click on the registration link.

iii. Fill in the required details, ensuring accuracy.

iv. Certain details such as mobile number and Aadhaar ID may be verified, if required.

v. Upon successful verification, the ABHA ID is generated and can be used for future healthcare services.

9. Medical Imaging & Remote Collaborations

Medical images play a key role in diagnosis and treatment. The majority of medical images captured from medical devices come in various file formats, including JPEG and DICOM. During diagnosis, radiologists and treating clinicians are required to perform imaging operations on medical images. Such operations allow them to obtain a clearer picture of clinical issues. A variety of independent tools are available in the market to perform imaging operations on medical images. However, it is considered good practice to provide such tools within the healthcare system, enabling images to be rendered on the fly and modified images to be saved for future reference.

In complex cases, clinicians need to discuss medical images with other clinicians to gain more clarity on patient conditions. Remote collaboration tools developed for performing imaging operations and annotations on medical images provide an edge in clinical decision-making.

Medical images are often large in size, ranging from megabytes (MBs) to gigabytes (GBs). These images require high bandwidth during exchange. Therefore, the underlying network must provide sufficient bandwidth to handle medical images smoothly. Similarly, imaging operations performed on medical images need to be transferred to the remote end in real time, generating a requirement for low network latency. In addition, data exchanged can be optimized to improve transmission efficiency.

Common operations performed on medical images include contrast control, brightness control, rotation by a certain degree, horizontal and vertical flipping, cropping, zooming in and out, resolution editing, annotation marking, tagging, freehand drawing, revert, and erasing.

C-DAC's Mercury™ Telehealth solution provides multiple features for image operations, enhancement, annotations, and support for multiple image formats (JPEG, PNG, etc.), including DICOM images. Reference images for browser-based imaging tools are shown below:

FIGURE 7: BROWSER BASED MEDICAL IMAGING-1

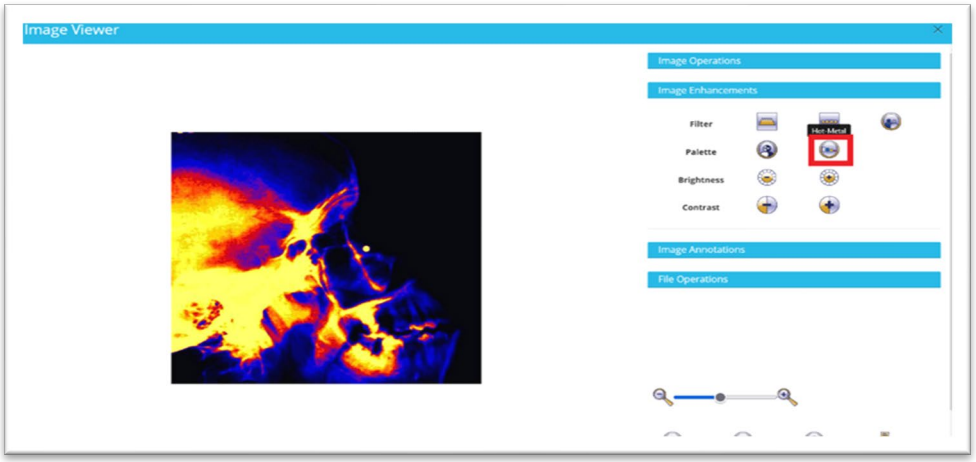
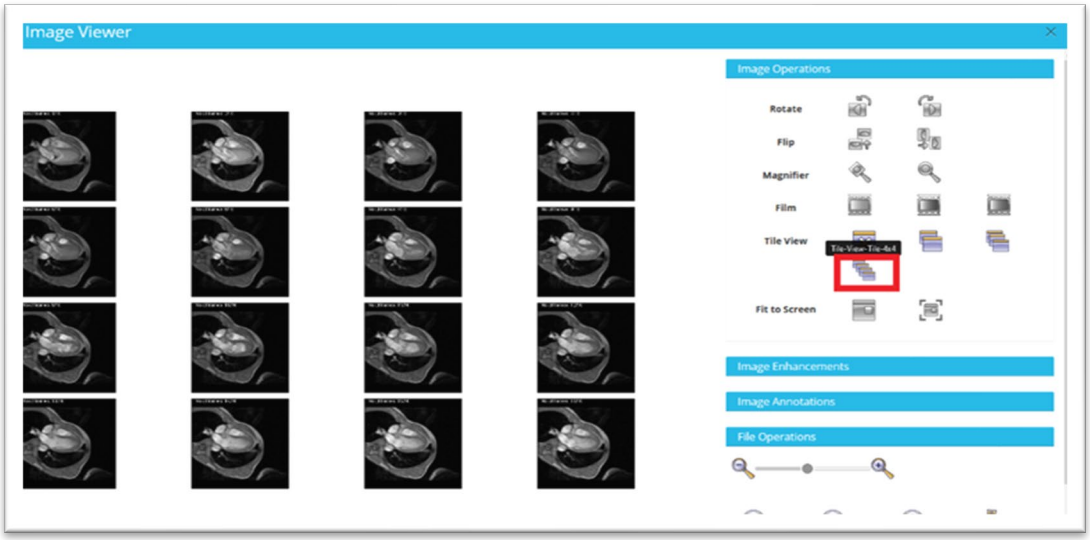


FIGURE 8: BROWSER BASED MEDICAL IMAGING-2



In C-DAC's Mercury™ Telehealth solution, a separate module is available for real-time image collaboration. Details of CollabMedImaging are as follows:

CollabMedImaging

Working towards the Digital India mission, C-DAC has developed the CollabMedImaging solution—a real-time collaboration service for medical images using the latest technologies. It connects remote physicians with specialists to discuss clinical cases through shared medical images. This technology enables the rapid exchange of medical images between healthcare providers and radiologists, regardless of physical location.

A typical workflow in CollabMedImaging involves simple steps. The clinician schedules a session with the required team. Once the session starts, the clinician securely shares medical images with other participants. Clinical conditions are discussed by marking annotations and performing imaging operations. Rendering of these operations occurs in real time and remains synchronized with audio-video communication. The updated images can be saved for future reference. The solution supports DICOM images, along with other image formats.

CollabMedImaging can also be used for continuous medical education and training programs to enhance learning experiences. It leverages the high bandwidth and low latency of 5G networks to deliver a rich and smooth user experience, even when handling large medical images.

FIGURE 9: COLLABMEDIMAHING FOR TELERADIOLOGY

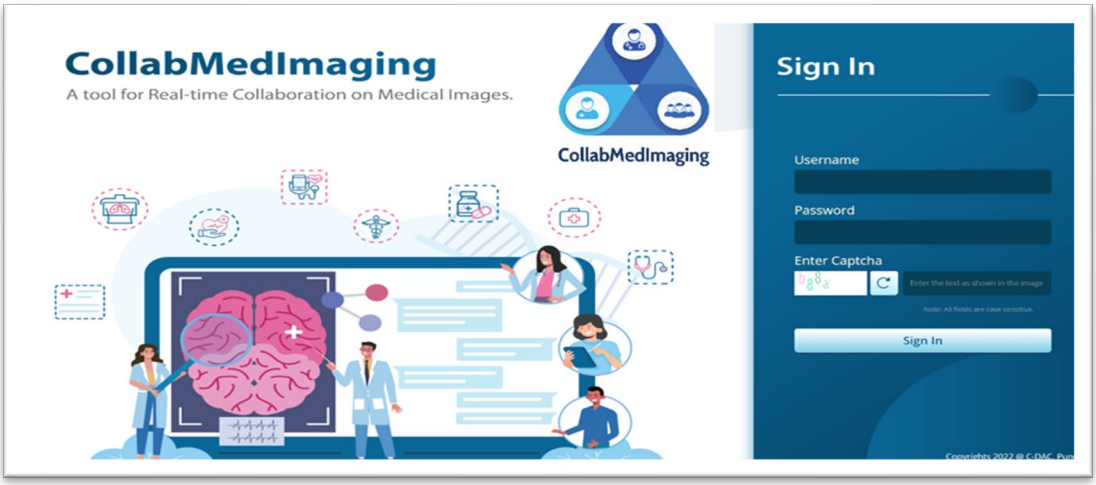


FIGURE 10: COLLABMEDIMAGING DASHBOARD

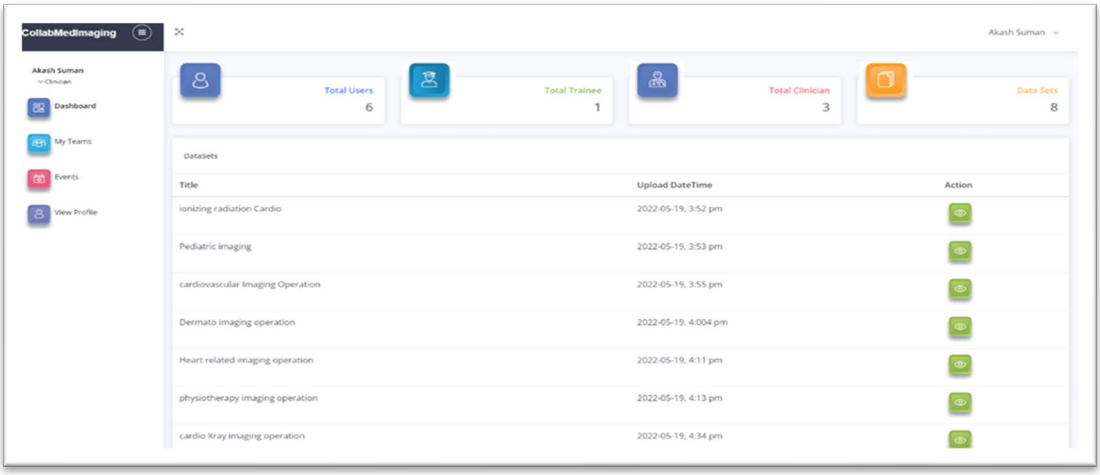


FIGURE 11: PHYSICIAN SHARING IMAGES WITH SPECIALIST

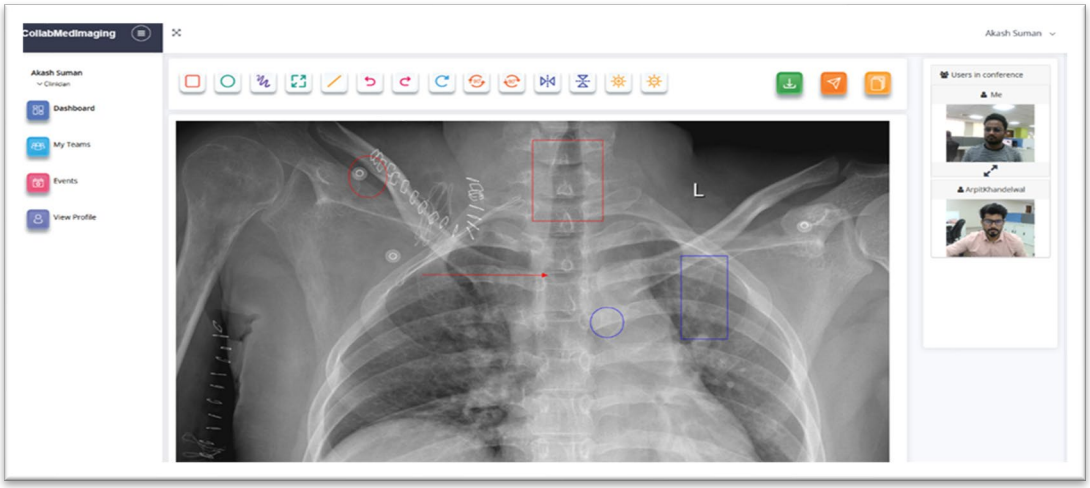
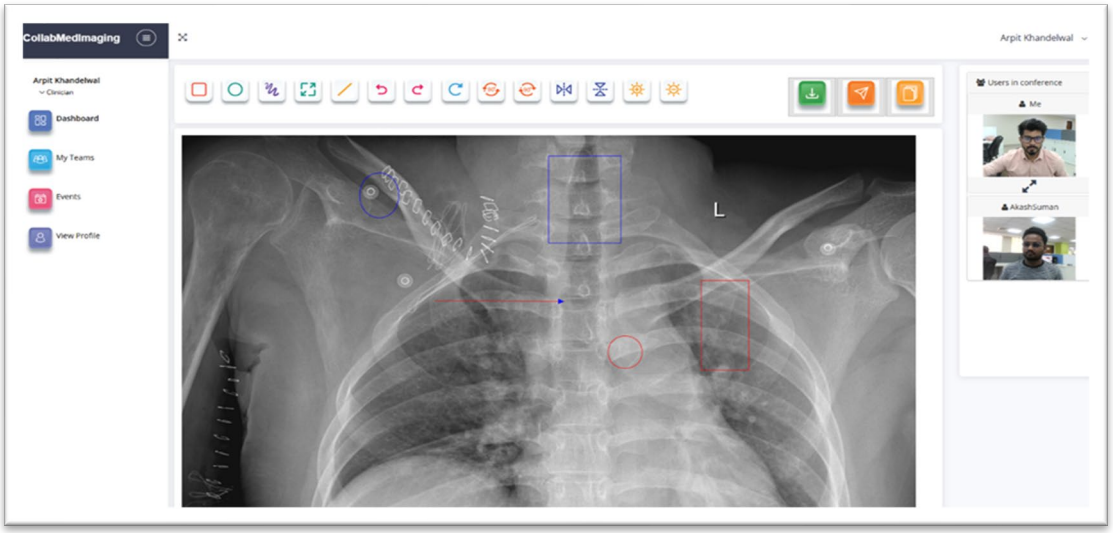


FIGURE 12: SPECIALIST GUIDING PHYSICIAN USING ANNOTATIONS & IMAGING



10. Cross-Cutting System Challenges

The digital transformation of healthcare in India presents multiple cross-cutting systemic challenges that span infrastructure, governance, workforce readiness, and regulatory maturity. These challenges are interconnected and require coordinated policy, technical, and institutional responses.

i. Infrastructure Disparities: Significant disparities persist between urban and rural regions in terms of broadband availability, hospital IT infrastructure, edge computing readiness, and reliable power supply. These limitations directly affect scalability of telemedicine, IoMT deployments, and 5G-enabled healthcare services.

ii. Workforce and Skill Gaps: Successful digital health adoption requires a trained clinical and technical workforce capable of operating digital systems, interpreting AI outputs, managing cybersecurity risks, and maintaining interoperable platforms. Limited digital literacy and insufficient structured training programs remain key barriers.

iii. Interoperability Limitations: Fragmented healthcare IT systems, inconsistent adoption of standards, and siloed data architectures restrict seamless data exchange and coordinated care delivery across institutions and platforms.

iv. Cybersecurity Maturity Gaps: Healthcare systems face increasing exposure to cyber threats, including ransomware, medical device vulnerabilities, and identity theft risks. Inconsistent implementation of structured risk management frameworks and Zero Trust architectures affects overall resilience.

v. Regulatory and Governance Uncertainty: Evolving regulations related to AI governance, data lifecycle management, digital consent, and cross-border data flows create uncertainty for healthcare providers and technology developers. Clear, harmonized regulatory frameworks are essential for sustained innovation and safe deployment

Addressing these systemic challenges requires coordinated action across standards development, regulatory harmonization, infrastructure investment, and capacity building initiatives.

11. Opportunities

AI doesn't replace clinicians - it amplifies their reach, especially where the system is stretched the most. Healthcare AI could be our most impactful leap yet.

Affordable, accessible, scalable AI-powered healthcare solutions have potential to augment frontline workers, automated X ray readings to assist in early diagnosis to support radiology and pathology workflows and deliver personalized care across geographies and languages. Audited by AI driven use cases to make systems more transparent and cut the fat bills.

If designed responsibly, with inclusivity, ethics, real-world constraints, Health AI can help bridge gaps between urban and rural care, prevention and treatment, demand and supply.

Capacity Building and Local Skill Enhancement Sustainable digital healthcare transformation requires parallel investment in human capacity building. Training of ASHA workers, rural healthcare operators, biomedical technicians, and telemedicine coordinators is essential for effective utilization of digital infrastructure. Skill enhancement initiatives must be aligned with regional healthcare needs to ensure technology adoption benefits the general population.

Despite these challenges, the convergence of healthcare and next generation networks offers substantial opportunities:

i. Improved access to healthcare services through telemedicine, remote diagnostics, tele-ICU, and mobile healthcare solutions for underserved populations.

ii. Enhanced quality of care and clinical decision-making enabled by real-time data access, AI-assisted analytics, medical imaging, and continuous patient monitoring.

iii. Efficient utilization of healthcare resources, including specialist expertise and critical infrastructure, through connected and virtual care models.

iv. Adoption of advanced technologies such as 5G network slicing, edge computing, digital twins, and immersive platforms to support latency-sensitive and mission-critical healthcare applications.

v. Strengthening of national digital health initiatives, including unified health identifiers, interoperable health information exchange, and cloud-based health platforms.

vi. Opportunities for innovation, standardization, and global alignment, supporting the evolution of sustainable digital healthcare models

vii. This is precisely where AI can make a transformative difference.

12. Recommendations

Based on the discussions across healthcare ecosystem aspects, digital infrastructure, security and privacy, 5G capabilities, immersive technologies, and regulatory considerations, the following observations and directions emerge:

i. There is a need to strengthen interoperability across hospital information systems, telemedicine platforms, medical devices, and IoT ecosystems by encouraging consistent use of common data models, interfaces, and messaging standards.

ii. Security and data privacy must be treated as foundational requirements for digital healthcare systems, with protection mechanisms integrated across devices, network, platform, and application layers.

iii. Data Management there is a need to strengthen secure, structured, and consent-based health data exchange mechanism within India's Digital health ecosystem. While significant progress has been made through initiatives such as the Ayushman Bharat Digital Mission (ABDM), ABHA-based digital identity, Unified Health Interface (UHI), and adoption of standards such as HL7 FHIR for health data exchange, uniform implementation across healthcare institutions remains inconsistent.

iv. The role of next generation networks, particularly 5G, is critical in enabling latency-sensitive and high-reliability healthcare use cases such as tele-ICU, remote patient monitoring, medical imaging, and connected ambulances. Network capabilities such as slicing and quality-of-service differentiation warrant focused consideration.

v. Digital infrastructure, including cloud and edge computing, reliable broadband connectivity, and health information exchange platforms, is essential for scalable deployment of digital healthcare services across diverse geographies.

vi. Emerging technologies such as digital twins and immersive platforms offer potential benefits for training, simulation, mental health support, and advanced care delivery; however, their adoption requires careful consideration of usability, data protection, and regulatory alignment.

vii. Regulatory frameworks and compliance mechanisms need to evolve in parallel with technological advancements to address data governance, medical device security, and cross-platform interoperability, while ensuring patient safety and trust.

viii. Capacity Building and Local Skill Enhancement Sustainable digital healthcare transformation requires parallel investment in human capacity building. Training of ASHA workers, rural healthcare operators, biomedical technicians, and telemedicine coordinators is essential for effective utilization of digital infrastructure. Skill enhancement initiatives must be aligned with regional healthcare needs to ensure technology adoption benefits the general population.

ix. Inclusive and Multilingual Digital Health Platforms Digital healthcare systems should incorporate multilingual interfaces, regional language teleconsultation capabilities, and accessible user design to ensure equitable healthcare access for underserved, rural, and semi-literate populations.

India has laid the foundation for healthcare standardization through Ayushman Bharat Digital Mission (ABDM) architecture, telemedicine guidelines, digital registries, and adoption of globally aligned interoperability standards. However, as the ecosystem evolves toward 5G-enabled, IoMT-integrated, AI-assisted, and edge-supported healthcare systems, standardization efforts must focus on conformance validation, device compliance frameworks, secure data exchange, and harmonized implementation across heterogeneous platforms to ensure scalable, secure, and interoperable national deployment.

13. Conclusion

The healthcare ecosystem is increasingly dependent on digital technologies and advanced communication networks to address challenges related to accessibility, quality of care, and operational efficiency. As discussed throughout this whitepaper, next generation networks combined with digital health technologies such as IoT-enabled medical devices, telemedicine platforms, remote patient monitoring, 5G connectivity, cloud and edge computing, and immersive technologies are redefining healthcare delivery models.

This whitepaper has examined healthcare from a communications and ICT perspective, covering healthcare ecosystem components, hospital information systems, security and data privacy, regulatory frameworks, and emerging technologies including digital twins and the metaverse. While national initiatives and technological advancements have accelerated digital healthcare adoption, the effective realization of these benefits depends on interoperability, secure infrastructure, regulatory clarity, and stakeholder collaboration. A holistic and standards-driven approach is therefore essential to build scalable, secure, and future-ready healthcare systems.

The future of healthcare lies in a fully connected, patient-centric ecosystem where digital platforms, intelligent systems, and secure communication networks seamlessly integrate to enable continuous care beyond hospital boundaries. A connected healthcare vision will support proactive disease management, equitable access in rural and underserved regions, data-driven clinical decision-making, and improved health outcomes. With responsible adoption of emerging technologies and strong governance frameworks, India is well positioned to build a scalable, secure, and inclusive digital health ecosystem for the coming decades.

Digital healthcare transformation must remain human-centric, ethically governed, and inclusion-driven, ensuring that technological advancement translates into equitable healthcare access across all regions of India and supports national Healthcare priorities under Viksit Bharat, aligned with initiatives such as Ayushman Bharat and the Ayushman Bharat Digital Mission.

.

Annexure - I

Detailed Telemedicine Deployments in India (Illustrative)

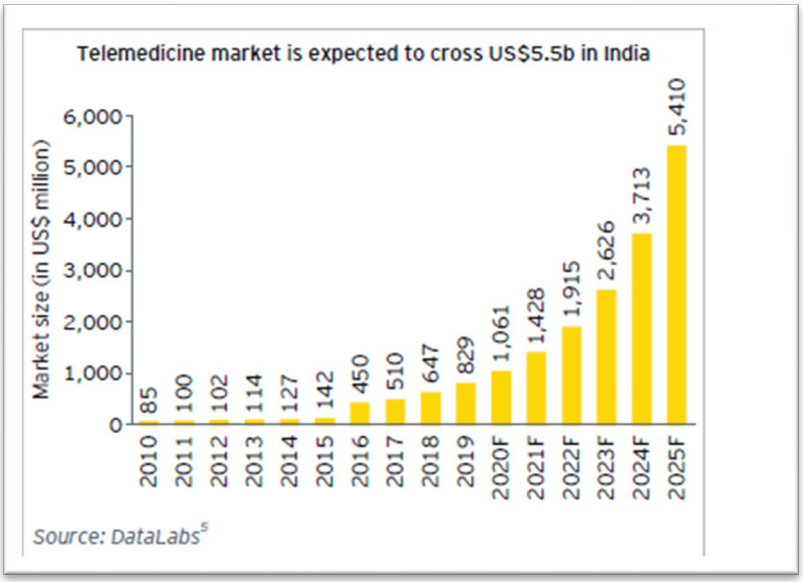
A. Early Telemedicine Initiatives

In India, several initiatives have been undertaken by both public and private sectors in initiating several telemedicine based remote healthcare delivery services. The very Iinitial efforts are were supported by technical ministries like Ministries of Electronic & Information Technology (MeitY) and Department of Space.

Indigenous technology development and pilot deployments were undertaken by Centre of Advanced Computing (C-DAC) and ISRO, pioneer in telemedicine in India (2001). These initiatives initially connected Apollo hospitals, Chennai, and Chittoor, dist. Andhra Pradesh, and provided telemedicine systems for 384 Hospitals, expanded to 15 super-speciality and 45 rural and remote hospitals. Satellite connectivity was also facilitated for 18 mobile telemedicine units in the country.

Similarly the such Through joint initiatives were taken by joint efforts of ISRO, the Ministry of Health and Family Welfare (MoHFW), MeitY, and the Government of India, telemedicine services were extended to remote locations such as Andaman and Nicobar, Lakshadweep Islands, Jammu & Kashmir, West Bengal, Tamil Nadu, and tribal areas in the north-eastern and central regions of the country.

Telemedicine market in India



There is an increasing trend of adoption of Telemedicine in India especially post COVID-19. The telemedicine market in India was expected to grow at a compound annual growth rate (CAGR) of 31% during the period 2020–25 and reach USD $5.5 billion. Due to pandemic, virtual care services, including teleconsultation, telepathology, teleradiology and e–pharmacy, have witnessed increased demand in India.

B. State-Level Telemedicine Networks (Illustrative List)

Some of these initiatives planed are mentioned in the below table:

TABLE 2: Telemedicine network of various states in India

State	Speciality Hospital besides several district hospitals
Jammu & Kashmir	Sher e Kashmir Institute of Technology
Himachal Pradesh	IGMC Shimla and PGIMER Chandigarh
Punjab	Government Medical College and Hospital and five some polyclinics of the state
Uttar Pradesh	SGPGIMS, Lucknow
Jharkhand	Some 3 Medical Colleges and Hospitals
West Bengal	School of Tropical Medicine, NRS Medical College &Hospital, Kolkata, Burdwan Medical College & Hospital, Burdwan
Rajasthan	6A number of State Medical Colleges
Northeastern States	Narayana Hrudayalaya, Bangalore
Odisha	3 Some Medical Colleges that further linked with SGPGIMS A number of 5 State Specialty Hospitals, 39 several district hospitals, and 13with eICU units under C-DAC's Odisha Telemedicine Network Using Mercury(™)
Chhattisgarh	Government Medical Colleges at Raipur &Bilaspur
Kerala	Amritha Institute of Medical Sciences, Kochi, Sri Chitra Medical Science and Technology, Tiruanantpuram,
Tamil Nadu	Sri Ramachandra Medical College and Research Institute, Chennai,
Karnataka	Narayana Hrudayalaya, Bangalore
Jammu & Kashmir	Paediatrics eICU at SMGS Hospital Jammu connecting 10 several Remotes Sites in Jammu

C. National Platforms Supporting Telemedicine

Indian players in Telemedicine e-Services:

Some of the examples Iin India including which started working in the telemedicine domain include, several private and public sector organizations have started working in telemedicine domain. Some are mentioned here: C-DAC (Pune, Mohali ,Thiruvananthapuram); Sanjay Gandhi Postgraduate Institute of Medical Sciences (SGPGI), Lucknow; Apollo Telemedicine Network Foundation, Hyderabad; Online Telemedicine Research Institute, Ahmedabad; Televital India, Bangalore; Vepro India, Chennai; Prognosys Medical Systems Pvt. Ltd., Bangalore; Medisoft Telemedicine Pvt. Ltd., Ahmedabad; diagnosis Technologies, Ahmedabad; Karishma Software Ltd., New Delhi; Neurosynaptic Communications Pvt Ltd., Karnataka; Amrita Institute of Medical Sciences (AIMS), Kochi, Kerala; Larsen & Turbo, Mumbai; West Bengal Electronics Industry Development Corporation Ltd., Kolkata; and Space Hospitals Ltd., Chennai.

Other notable organisations include Amrita Asia Heart Foundation (AHF), Narayana Hrudayalaya, Bangalore; Escorts Heart Hospital; Fortis; and Sir Ganga Ram Hospital (SGRH), New Delhi.

Telemedicine services in India:

There are several telemedicine services available in India which are launched by Government as well as by private agencies. The few services are mentioned below:

i. eSanjeevani (e-consultation platform)
   i). Implemented across 28 states and 8 union territories. It supports doctor-to-doctor and patient-to-doctor tele-consultation and has enabled over couple of hundred 160 million tele-consultations nationwide.
   ii). Provide medical education to interns, people at Common Service Centers (CSCs), etc. – MeitY and CDAC.

ii. Swasth App: (Launched in June 2020)
   i). Swasth App is a mobile-based digital health platform that facilitates free telemedicine consultations for users.
   ii). The app acts as a health services aggregator, guiding patients to multiple service options such as booking diagnostic tests, ordering medicines online, requesting home healthcare services, and locating nearby hospitals with information on bed availability.
   iii). About 100 leading hospitals, health tech start-ups developed this app.

iii. AYUSH Sanjivani' App (Launched in May 2020)
   i). This App was developed by Ministry of AYUSH and MeitY.
   ii). The app aims to collect and analyze data on the acceptance, adoption, and usage of AYUSH-based health practices and preventive measures among the population.
   iii). It was designed to reach approximately 50 lakh users, supporting evidence-based assessment of AYUSH interventions.

Medical Tourism:

The advent of electronics and information technology in medical devices / health care has made a meaningful impact on the healthcare system, attracting the tourists from different parts of the world. Medical tourism is increasing in India, and the country is emerging as a preferred healthcare destination for neighbouring and far-off countries.

Therefore, the use of Telemedicine and e-health tools has the potential to facilitate the exchange of electronic health information between hospitals globally. The Ministry of External Affairs deployed telemedicine projects in African subcontinent, SAARC region, and Central Asia, which have facilitated telecare services, particularly follow-up care after initial treatment in India.

Many corporate hospitals in India have integrated telemedicine services for their overseas clients as a routine practice.

Government initiatives

The Indian government has put forth several initiatives and policies aimed at delivering healthcare services remotely and efficiently. These include:

The Government of India's recently announced (15th Aug 2020) National Digital Health Mission (NDHM) opens the door for universal digital healthcare system in the country. The Government's Bharat broadband network programme, aimed at connecting every corner of the country through the

National Optical Fibre Network (NOFN) for internet connectivity, is another important initiative which will help in deployment of nationwide telemedicine services.

National and state level telemedicine networks aim to connect to the remote areas by upgrading existing Government healthcare facilities through the creation of a reliable, ubiquitous, and high-speed network backbone. SATCOM based telemedicine nodes at Pilgrim Places are being deployed to reach geographical remote and inaccessible locations.

The National Medical College Network, under which 50 Government medical colleges are being inter-linked for tele-education, e-learning, and online medical consultations using the National Knowledge Network (NKN).

The Ministry of Health and Family Welfare (MoHFW) has also issued Telemedicine guidelines, enabling the practice of healthcare delivery services remotely. Niti Aayog has proposed the National Health Stack (NHS), a nationally shared digital infrastructure to support the healthcare ecosystem. It aims to enable the entire population-scale health management and research through a national health analytics platform leveraging Big Data and AI/Machine Learning (ML).

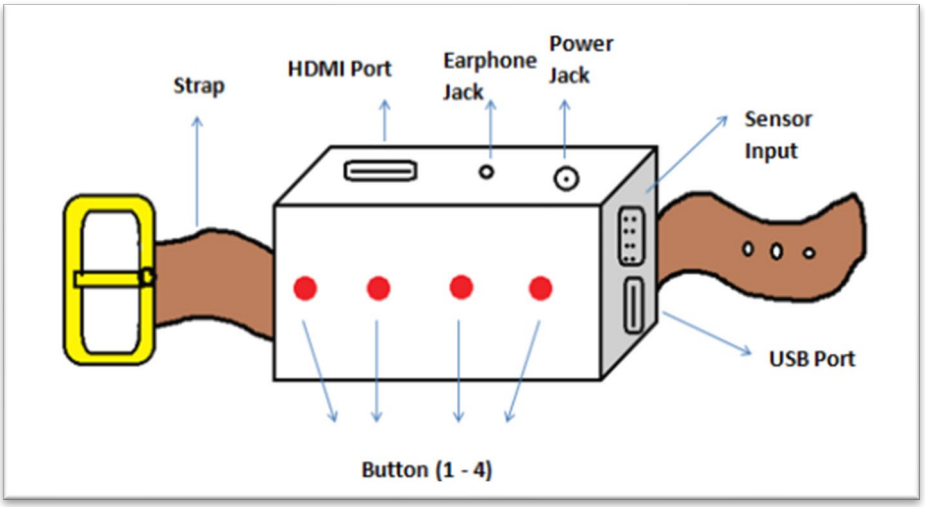
The objective of National Health Stack is to seamlessly link the healthcare providers, payers and service delivery agencies to national health electronic registries, reduce costs through shared digital infrastructure, and promote population-wide wellness. The digital infrastructure will be owned and operated by the government and will be accessible through open APIs.

Annexure - II

SMART JACKET & SMART CANE: TECHNICAL ARCHITECTURE AND HARDWARE DETAILS

This annexure provides detailed hardware specifications and implementation-level descriptions of the Smart Assistive Wearable System.

FIGURE 13: WEARABLE CONTROL BOX



The proposed system is an Electronic Travelling Aid (ETA), a wearable assistive device that comprises a control box mounted on the arm of the jacket (see Fig. 5). The various components of the control box are as follows:

i. Strap - It is used to source the control box on the arm of a person wearing a jacket.

ii. HDMI (High-Definition Multimedia Interface) Port - It provides an audio/video interface for transmitting data. The HDMI standard was developed by multiple companies, including Hitachi, Philips, Sony, and Toshiba. A single HDMI cable replaces three composite audio/video cables, making it easier to connect two devices together for transmitting audio and video signals. HDMI is capable of transmitting standard, enhanced, and high-definition video signals, as well as up to 8- channels of digital audio.

iii. USB (Universal Serial Bus) Port - It is a standard connection interface that allows digital data transfer. USB ports rated at 5 V and 2.5 A are additionally provided for charging personal devices. USB connectors come in different shapes and sizes. Most USB connector types, including standard USB, Mini USB, and Micro USB, have two or more variations of connectors.

iv. Button (1-4) - A Push Button is a type of switch that completes the circuit when pressed. It is commonly used to trigger the systems functions. A spring mechanism allows the button to return to its initial (off) position once released. These buttons are typically made of plastic or metal and serve the purpose of selecting various assisting features. Two additional buttons are provided for switching the operating system (OS) and main power supply

v. Earphone Jack - A 3.5 mm audio jack that allows connection of headphones or speakers for audio output.

vi. Power Jack - Power connectors allow an electrical current to supply power to the device This jack is used for charging the system battery.

vii. Sensor Input - All ultrasonic sensors are attached to the control box using an FRC (Flat Ribbon Cable) connector.

System features:

i. Detection of Object's Range

ii. Detection of Object's Height

iii. On-Demand Cab Booking Facility

The system will activate the GPS module when the user presses the third button on the control box.

i. Emergency Contact: If the visually impaired person loses orientation or requires assistance, pressing the fourth button triggers the GPS module. The latitude and longitude coordinates are converted into a Google Maps link and shared with relatives or known contacts.

ii. Detection of Water: The system includes a water detection mechanism integrated into the white cane to identify wet surfaces and water-filled potholes. Upon detection, an audio alert is generated to warn the user, helping prevent slips and enhance safety during navigation.

iii. Relocating White Cane: When the user loses contact with the cane, the pressure on the leaf switch changes. The leaf switch activates upon minor pressure variation and generates a signal that is sent to the Arduino-based microcontroller unit. The microcontroller then activates a buzzer, enabling the user to locate the cane.

FALL DETECTION:

One of the common issues faced by visually impaired individuals is injury resulting from falls, some of which may lead to fatalities. Therefore, an effective fall detection algorithm is required to reduce response and rescue time.

This issue is addressed using a threshold-based detection algorithm that checks whether specific parameters exceed predefined threshold values within a given time interval. In a fall scenario, there is a sudden and significant change in acceleration, followed by a period during which the person remains motionless, indicating no change in orientation. These characteristics form the basis of the proposed algorithm.

Initially, data is collected from the accelerometer, and the acceleration magnitude is calculated. While acceleration represents the rate of change of velocity, the acceleration magnitude indicates the intensity of motion, which is critical for fall detection. The parameters ax, ay, and az represent acceleration along the X-, Y-, and Z-axes, respectively.

After calculating the acceleration magnitude, the algorithm checks whether the value exceeds a predefined lower threshold, which then gradually increases towards a higher threshold. The system verifies whether the higher threshold is crossed within a short time window (for example, 500 ms). If this condition is satisfied, the algorithm further checks for a change in orientation within the same time interval. Subsequently, it verifies whether the orientation remains unchanged for a certain duration, confirming that a fall has occurred.

If any of the conditions fail, the algorithm resets and restarts, ensuring continuous monitoring.

Annexure - III

eSANJEEVANI – NATIONAL TELEMEDICINE SERVICE

Background:

eSanjeevani is India's National Telemedicine Service implemented by the Ministry of Health and Family Welfare (MoHFW) to provide free, equitable, and remote healthcare access across the country through structured video-based clinical consultations.

It was conceptualised to address systemic challenges such as shortage of doctors at the primary care level, uneven access to specialized services in rural regions, lack of electronic health record creation, and gaps in continuity of care. By leveraging digital infrastructure, eSanjeevani enables patients and providers to connect through telemedicine irrespective of physical distances.

Service Models

eSanjeevani operates through two complementary service delivery models:

i. Provider-to-Provider (Assisted) Model – eSanjeevani AB-HWC: This model connects Health & Wellness Centres (HWCs) and community health officers (CHOs) with doctors and specialists located at higher-level facilities using a hub-and-spoke architecture. It enables assisted teleconsultations for patients who visit local primary centres.

ii. Patient-to-Provider (Direct) Model – eSanjeevani OPD: This model enables patients with internet-enabled devices to receive direct outpatient teleconsultations from doctors and specialists in the comfort of their homes via audio-video sessions.

Operational Scale and Reach

As of late 2024 / early 2025:

i. eSanjeevani has served over 330 million patients nationally since its launch, making it one of the world's largest telemedicine implementations.

ii. The platform operates through a vast network of health facilities, hubs and spokes, including:

   i). Approximately 1,31,000+ health facilities serving as spokes (AB-HWCs),

   ii). 16,000+ hub facilities providing specialist connections, and

   iii). Hundreds of online OPD channels serving direct patient consultations.

iii. The network includes more than 230,000 registered healthcare providers offering services across general and specialist domains.

Key Features and Enhancements

To improve robustness, scalability, and usability, eSanjeevani has evolved with multiple enhancements:

i. Cloud-based architecture for seamless scaling and high availability.

ii. Multilingual interface to support users in various Indian languages.

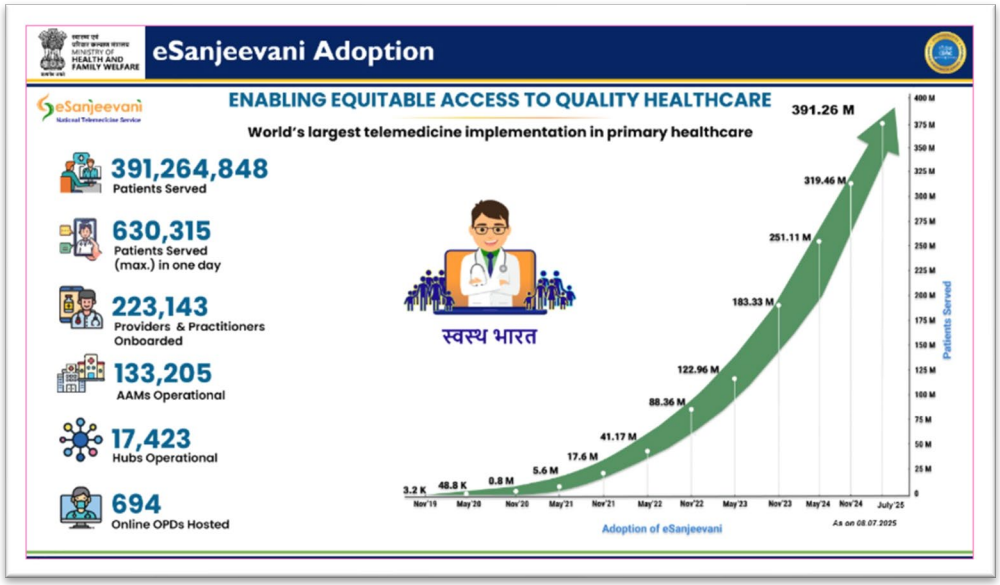
iii. Responsive and flexible video consultation design to support diverse device formats.

iv. Integration with digital health identifiers such as ABHA ID and Health Professional/Facility registries for coordinated health data linkage.

v. Features such as real-time sharing of records, follow-up tagging, and unified dashboards to enhance continuity of care and data quality.

Strategic Impact

eSanjeevani has contributed significantly to improving equitable healthcare access by facilitating telemedicine services for millions of individuals, especially in rural and underserved areas. Its nationwide adoption has helped reduce travel burden, eased congestion in secondary and tertiary facilities, and strengthened primary care delivery through digital connectivity.



Annexure - IV

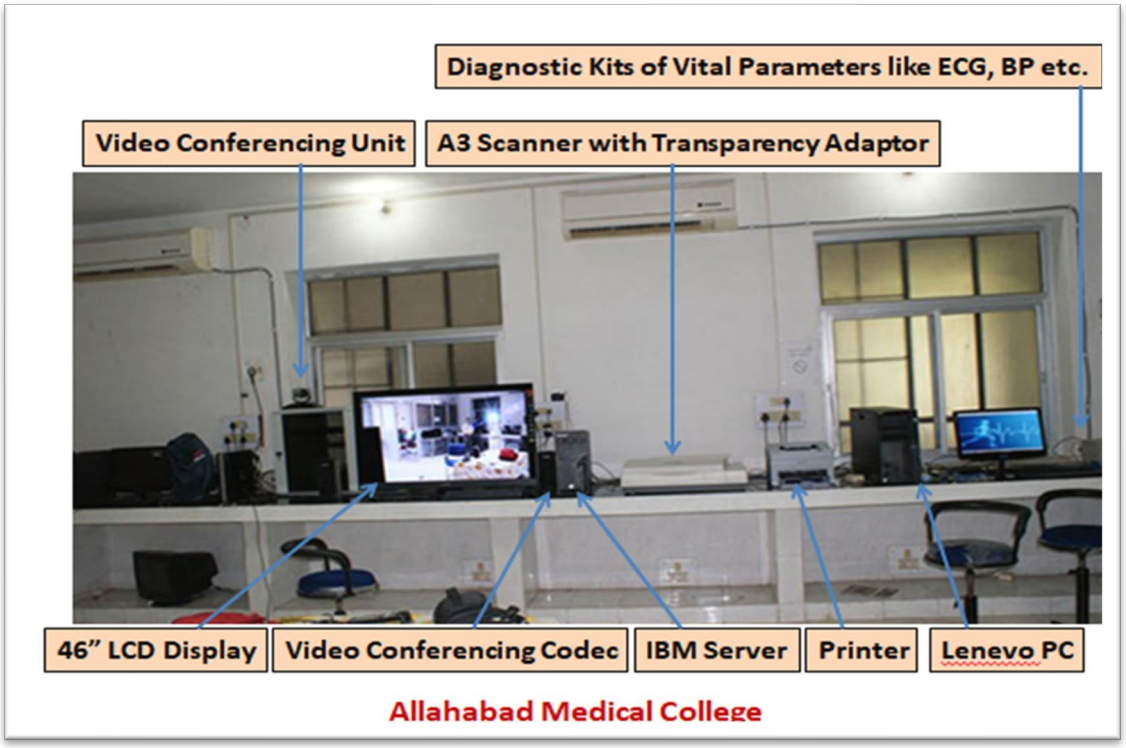
SANJAY GANDHI POSTGRADUATE INSTITUTE OF MEDICAL SCIENCES (SGPGIMS) TELEMEDICINE HUB

Annexure – V

SANJAY GANDHI POSTGRADUATE INSTITUTE OF MEDICAL SCIENCES (SGPGIMS) TELEMEDICINE HUB

Annexure – VI

DIGITAL MEDICAL LIBRARY



Annexure – VII

Illustrative Telemedicine Deployment Scenarios

This annexure provides illustrative deployment scenarios of telemedicine systems highlighting infrastructure requirements, connectivity models, and operational workflows. These scenarios are indicative and intended to support understanding of practical implementation approaches.

Annexure – VIII

TELEMEDICINE BUS OUTSIDE & INSIDE

Annexure – IX

National Thermal Power Corporation (NTPC) Kiosk Platform

Annexure -X

C-DAC's Mercury™ Telehealth Solution

C-DAC's Mercury™ Telehealth Solution is an enterprise-grade 5G & cloud-enabled comprehensive EMR / EHR, TeleICU and Telemedicine solution. The developed solution by C-DAC is highly available, scalable and secure with a user-friendly interface to carry out day to day clinical record keeping and tele-consultation operations. Coupled with cloud infrastructure, C-DAC's Mercury™ Telehealth Solution offers a low cost, highly maintainable solution for healthcare deprived citizens of the nation dwelling in remote areas. Components of Mercury™ are as follows:

i. Mercury™ on Cloud
ii. Mercury™ Remote Module
iii. Mercury™ for Android
iv. Mercury™ Cloud Repository
v. Mercury™ for Real-time Collaboration on Medical Images
vi. Mercury™ for VR Education & Training Platform

C-DAC's Mercury™ Telehealth Solution can be used in telemedicine scenarios like patient to doctor, doctor with multiple clinics, groups of clinicians, clinicians with specialist end and hospital-to-hospital interaction. The solution is deployable as an all-in-one virtual instance or use cloud persistent model for database and storage. This solution is also deployable over Local Servers / Data Centers.

Few glimpse of C-DAC's Mercury™ Telehealth Solution are as follows:

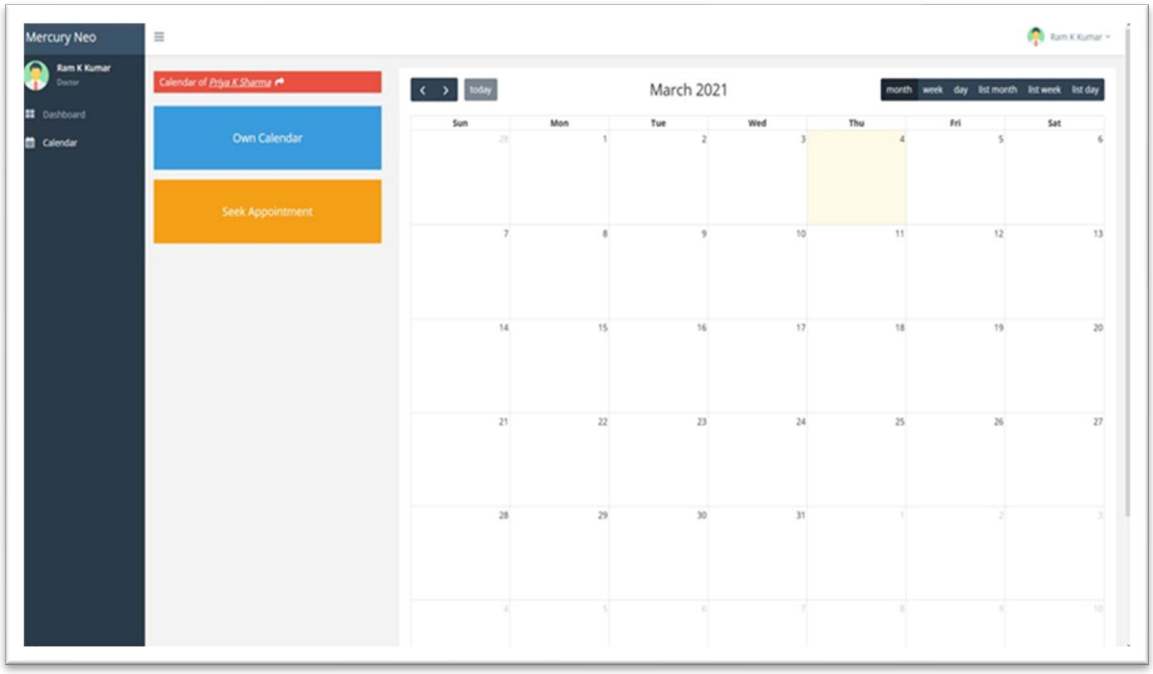


Figure 1 Scheduling- Calendaring

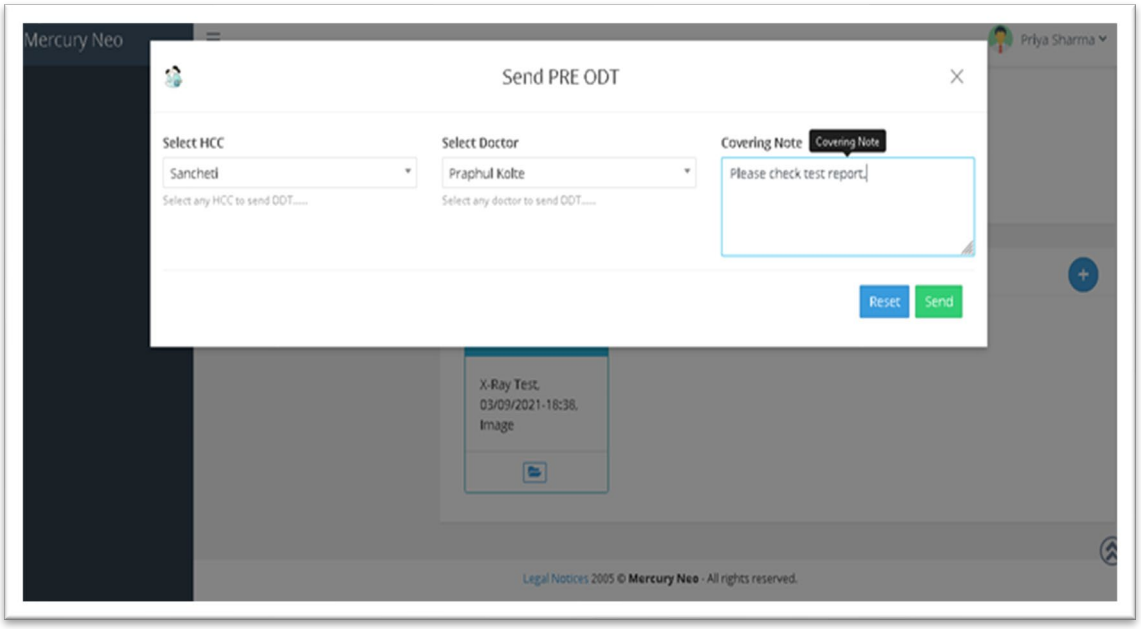


Figure 2 Offline Data Transfer

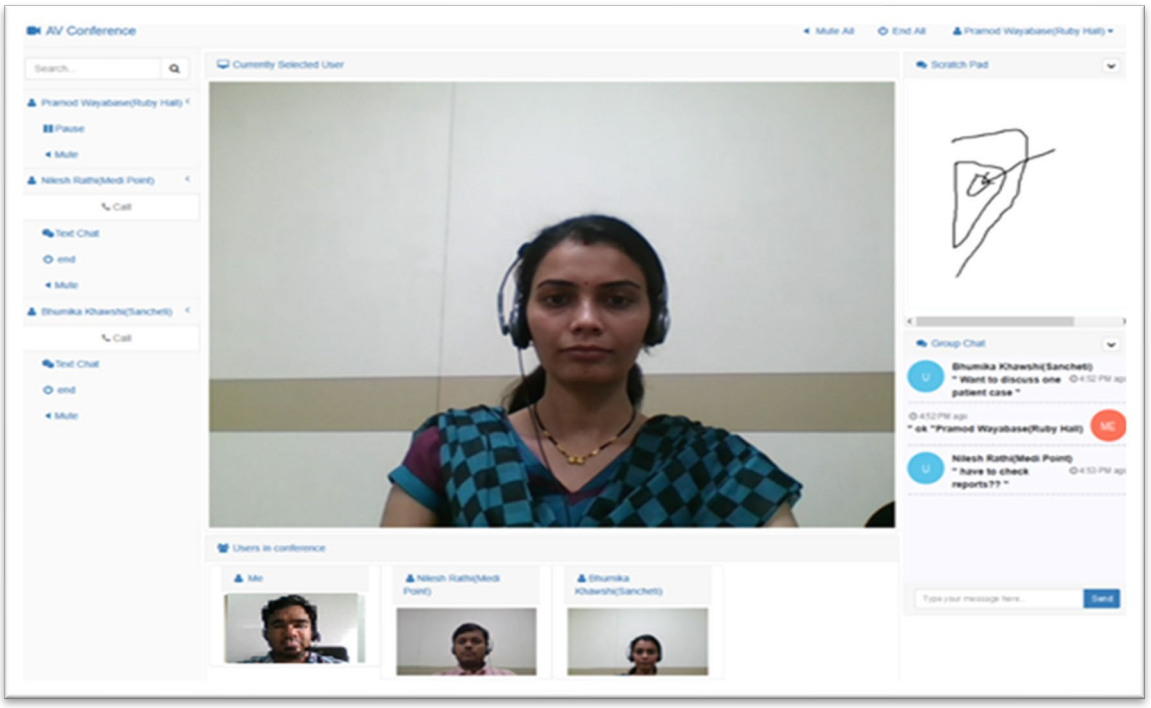


Figure 3 Integrated Audio-Video Conferencing

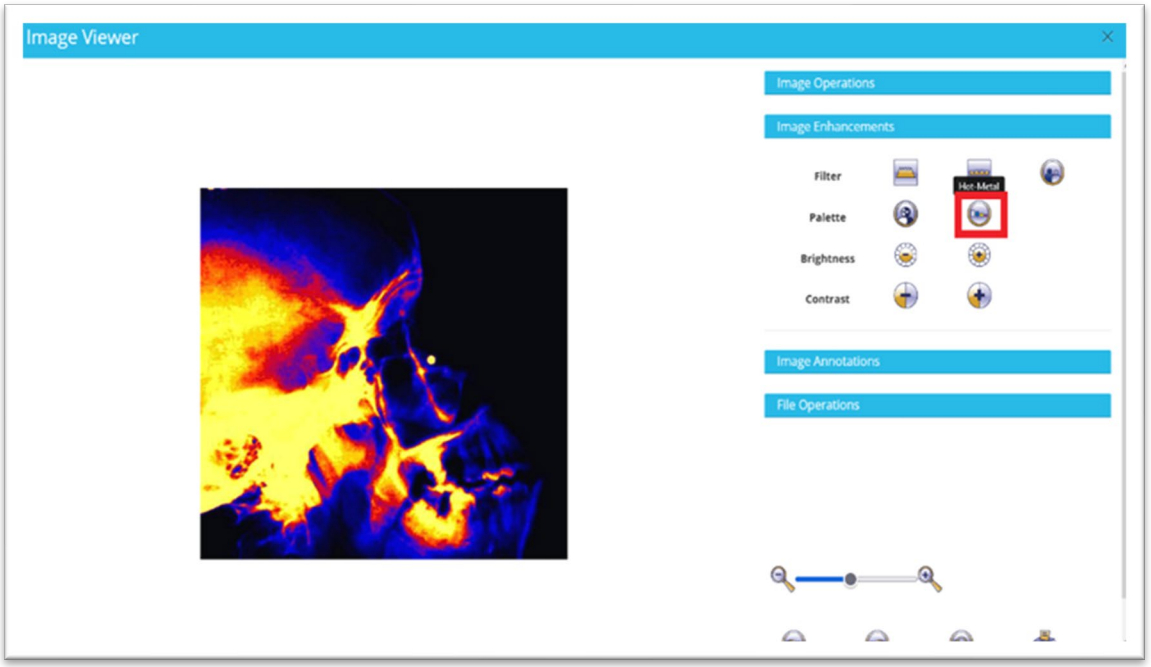


Figure 4 Browser Based Medical Imaging-1

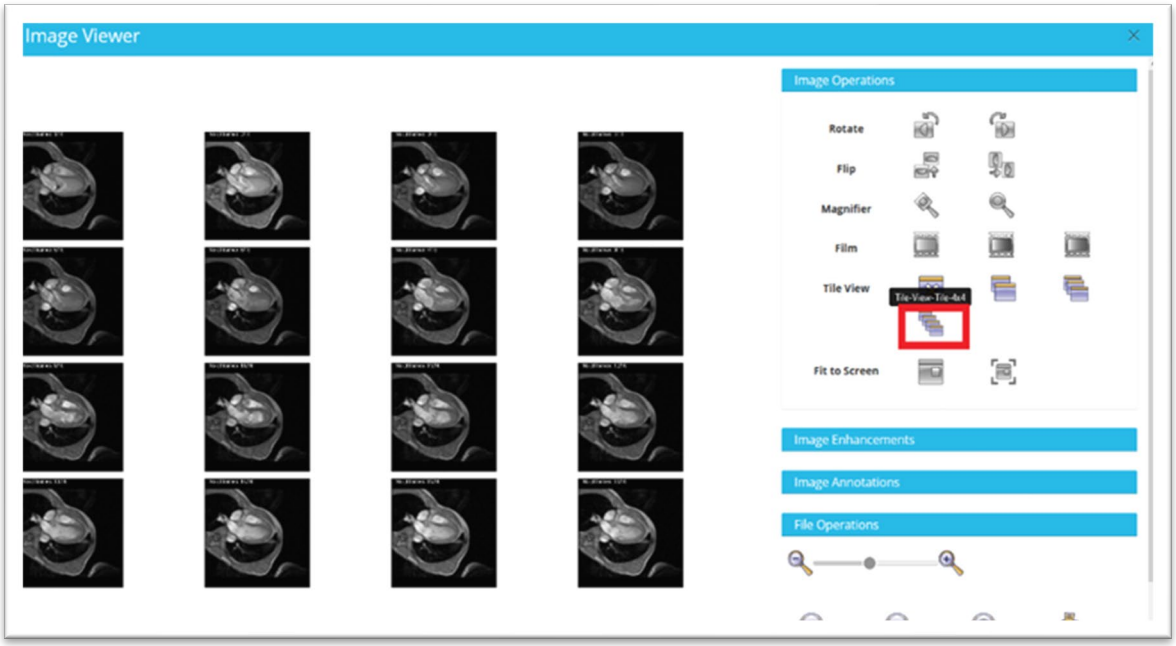


Figure 5 Browser Based Medical Imaging-1

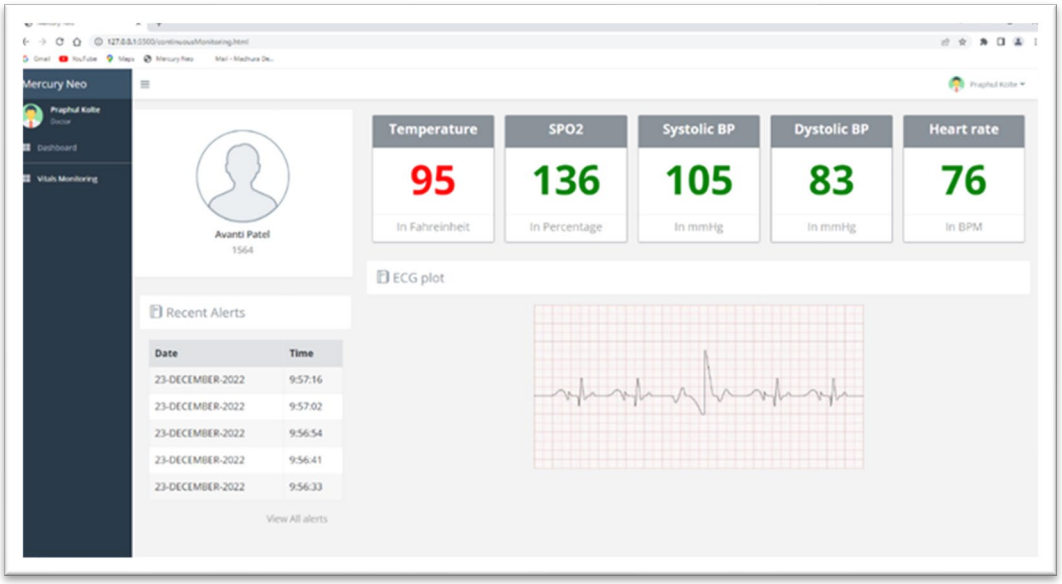


Figure 6 Patient ICU dashboard with Vitals & ECG

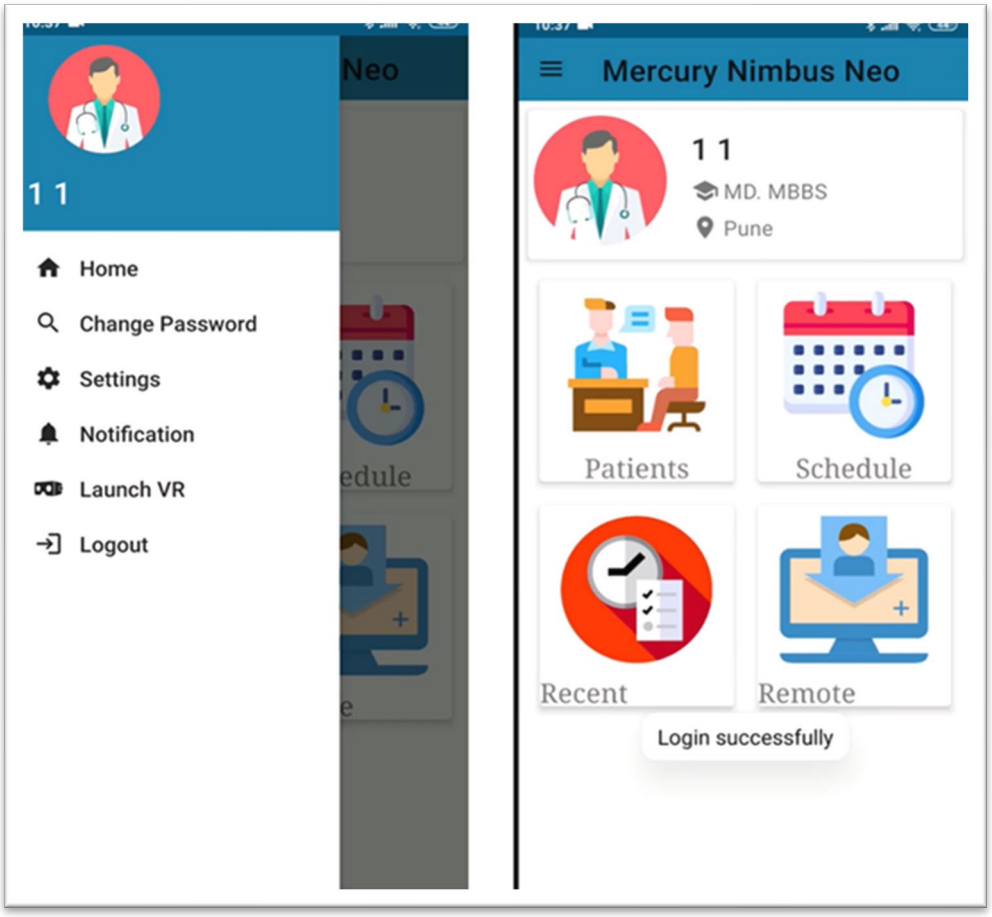


Figure 7 Android Application

References

This whitepaper draws upon peer-reviewed journal publications, international conference proceedings, national telemedicine workshops, government policy documents, international standards, institutional technical reports, and recognized industry reports. Detailed bibliographic references are maintained in the internal master reference repository and are available upon request.

Standards and Technical Specifications

1. International Organization for Standardization, ISO/TS 22220:2011 – Health Informatics — Identification of Subjects of Health Care.
2. International Organization for Standardization, ISO 18308:2011 – Health Informatics — Requirements for an Electronic Health Record Architecture.
3. International Organization for Standardization and Health Level Seven International, ISO/HL7 10781:2015 – Electronic Health Record System Functional Model.
4. International Organization for Standardization, ISO 27789:2013 – Health Informatics — Audit Trails for Electronic Health Records.
5. International Organization for Standardization, ISO/TS 14441:2013 – Health Informatics — Security and Privacy Requirements for Electronic Health Records.
6. Health Level Seven International, HL7 Version 2.x Messaging Standard.
7. Health Level Seven International, Fast Healthcare Interoperability Resources (FHIR) Standard.
8. Digital Imaging and Communications in Medicine (DICOM) Standard, National Electrical Manufacturers Association.
9. Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT).
10. Logical Observation Identifiers Names and Codes (LOINC).
11. International Classification of Diseases (ICD), World Health Organization.
12. Transport Layer Security (TLS) Protocol, Internet Engineering Task Force.
13. Datagram Transport Layer Security (DTLS) Protocol, Internet Engineering Task Force.
14. Data Distribution Service (DDS) Security Specification, Object Management Group.
15. Third Generation Partnership Project, The 5G Standard Specifications.

Government Policies and Regulatory Frameworks

16. Government of India, Information Technology Act, 2000.
17. Government of India, Digital Personal Data Protection Act, 2023.
18. Government of India, Proposed Digital Information Security in Healthcare Act (DISHA).
19. Government of India, Assisted Reproductive Technology (Regulation) Bill, 2020.
20. Government of India, Right to Erasure and Right to be Forgotten provisions under Data Protection Frameworks and related judicial interpretations.
21. Parliament of India, Lok Sabha Debates and Parliamentary Proceedings relating to Data Protection and Digital Health Legislation.
22. National Institute of Standards and Technology, United States Department of Commerce, Internal Report 8228 – Considerations for Managing Internet of Things Cybersecurity and Privacy Risks.
23. Internet Engineering Task Force, Request for Comments 7925 – Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things.

24. United Nations Global Working Group on Big Data, Handbook on Privacy Preserving Techniques for Statistical Disclosure Control.
25. World Health Organization, Ethics and Governance of Artificial Intelligence for Health: WHO Guidance, 2021.
26. World Health Organization, Global Health Observatory Data Repository Publications.
27. Ministry of Health and Family Welfare, Government of India, Telemedicine Practice Guidelines
28. Ministry of Health and Family Welfare, Government of India, National Digital Health Mission – Health Data Management Policy.
29. Ministry of Health and Family Welfare (MoHFW), Government of India, "eSanjeevani – National Telemedicine Service

Technical Reports and Institutional Publications

30. Telecommunications Standards Development Society, India, Technical Report "Study on system requirements related to Metaverse use cases in mobile network" TSDSI TR 6031.
31. Telecommunications Standards Development Society, India, Technical Report "Study on Semi-Autonomous Collaborative Telerobotics" TSDSI TR 6035.
32. Telecommunication Engineering Centre, Government of India, Technical Report on Machine-to-Machine Health Monitoring Framework.
33. Centre for Development of Advanced Computing, Mercury™ Telehealth Solution Documentation.
34. Indian Council of Medical Research, Digital Health and Research Publications.

Industry and Market Reports

35. Grand View Research, Digital Health Market Size, Share and Trends Analysis Report.
36. Market Research Future, Healthcare in Metaverse Market Research Report.
37. United Nations Children's Fund (UNICEF), Digital Health and Child Health Reports.
38. World Health Organization, Fact Sheets and Global Health Statistics Publications.
39. Hindustan Times, News Reports and Publications on Digital Health and Telemedicine Developments.
40. The Times of India, News Reports on Healthcare Technology and Digital Infrastructure.
41. United States Department of Health and Human Services, Public Statement on Cybersecurity Incidents Affecting Healthcare Systems.
42. UnitedHealth Group Incorporated, Official Statement on Change Healthcare Cybersecurity Incident.
43. Inc42 Media, Reports on Digital Health Startups and Health Technology Ecosystem in India.

International Journal Articles & Peer-Reviewed Publications

44. Qureshi et al., Article published in the journal *Healthcare*, Multidisciplinary Digital Publishing

Institute, 2022.

45. Qureshi et al., Article published in *IEEE Access*, Institute of Electrical and Electronics Engineers, 2021.
46. Ahad, Md. Atiqur Rahman and Yau, Kok-Lim Alvin, Article published in *IEEE Access*, Institute of Electrical and Electronics Engineers, 2019.
47. Li, C. Z. et al., Article published in the journal *Healthcare (Basel)*, Multidisciplinary Digital Publishing Institute, 2021.
48. Usmani et al., Article published in *General Psychiatry*, BMJ Publishing Group, 2022.
49. Park et al., Article published in *Frontiers in Psychiatry*, Frontiers Media SA, 2019.
50. Loucif et al., Article published in the *Journal of Computer and Communications*, Scientific Research Publishing, 2021.
51. Ma, Jingni et al., Article published in *EXPLORE: The Journal of Science and Healing*, Elsevier, 2023.
52. ZenVR, Paper presented at the *CHI Conference on Human Factors in Computing Systems*, Association for Computing Machinery, 2022.
53. Articles published in the *Journal of Telemedicine and Telecare*, SAGE Publications.
54. Articles published in the *Indian Journal of Critical Care Medicine*, Indian Society of Critical Care Medicine.
55. Tele-Intensive Care Unit study published in the Journal of the American Medical Association (JAMA).
56. Reynolds et al., Article published in *Telemedicine and e-Health*, Mary Ann Liebert, Inc., Publishers.
57. Articles published in the *Journal of Telemedicine and e-Health*, Mary Ann Liebert, Inc., Publishers.
58. Articles published in peer-reviewed Bioinformatics Journals including international publications in Computational Biology and Biomedical Informatics.
59. Articles published in *Open Bioinformatics Journal* and *Online Journal of Bioinformatics*.

Books & Book Chapters

60. Telemedicine in Surgery. In: Roshan Lall Gupta's Recent Advances in Surgery; Ritesh Agarwal, Saroj Kumar Mishra. (2013). New Delhi: Jaypee Brothers Medical Group Publisher Private Limited, Pages 263–277.
61. mHealth4U: Convergence of Information and Communication Technology and Mobile Technologies for Rural Healthcare Delivery. Repu Daman Chand, Indra Pratap Singh, Saroj Kanta Mishra. (2015). In: Public Health in India: Technology, Governance and Service Delivery, Pages 97–104.
62. Tele-mentoring in India: Experience with Endocrine Surgery. Saroj Kanta Mishra, Puthen Veettil Pradeep, Anjali Mishra. Chapter 11. Telehealth in the Developing World. ISBN 978-1-

85315-784-4, Pages 109–118, 2008.

63. Teleneurology: Past, Present and Future. Usha Kant Misra, Jayantee Kalita. Chapter 24. Telehealth in the Developing World. ISBN 978-1-85315-784-4, Pages 252–261, 2008.
64. Telemedicine in Developing World: Experience at Sanjay Gandhi Postgraduate Institute of Medical Sciences, Lucknow – A Tertiary Care Academic Medical Center. Lily Kapoor, Repu Daman Chand, Indra Pratap Singh, Saroj Kanta Mishra. Chapter 13. Telemedicine Concepts and Applications. The ICFAI University Press. ISBN 978-81-314-2089-8, Pages 151–160, 2008.
65. Telementoring in Endocrine Surgery. Saroj Kanta Mishra, Anjali Mishra, Puthen Veettil Pradeep. Chapter 11. Telesurgery Book. Edited by Shafi Ahmed Kumar and Jacques Marescaux. Springer-Verlag GmbH, Heidelberg, Germany. ISBN 978-3-540-72998-3, 2007.
66. E-Health – India Case Report. Saroj Kanta Mishra. “Making Better Access to Healthcare Services.” Published by International Telecommunication Union, Geneva. ISBN 4-87739-120-7, Pages 164–180, October 2005.
67. Application of Telemedicine in Surgery. Saroj Kanta Mishra. In: Telemedicine Manual. Published by Indian Space Research Organization, Bangalore. First Edition, Pages 83–90, 2005.

List of Contributors

TSDSI acknowledges the contributions of all the contributors, supporters, and other members of the IoT/M2M TRIP Forum, whose efforts have been instrumental in the success of this initiative. The work was chaired by Suresh V (C-DAC) and Abhishek Thakur (IDRBT), with the whitepaper championed by Prof. S. K. Mishra (Professor, Dept of Endocrine Surgery, Dr. RMLIMS, Lucknow & Distinguished Visiting Professor, IIT Kanpur) and supported by several dedicated individuals and the TSDSI Secretariat. Their combined expertise and collaboration have significantly enriched the process, and we are grateful for their valuable contributions.

S No	Name	Affiliation
1	S K Mishra	Dr. RMLIMS, Lucknow & IIT Kanpur
2	Arzad Alam Kherani	IIT Bhilai
3	Anuradha Kanamarlapudi	GE healthcare
4	Dr Gayatri Sakya	JSS Academy of Technical Education Noida
5	Dr Joy Mammen	CMC, Vellore
6	Dr Shashi Kant Pandey	SETS India
7	Hemant Jeevan Magadum	CDAC Trivandrum
8	Koushlendra Singh Sisodiya	Uniconverge Technologies
9	Navpreet Singh	IIT Kanpur
10	Pranav Singh	IDEMIA
11	Priyanka Bagade	IIT Kanpur
12	Priyesh Ranjan	CDAC Noida
13	Prof Raman Saxena	IIIT Hyderabad
14	Reshmi TR	SETS India
15	Rishabh Kumar	Uniconverge Technologies
17	Shailendra Singh Narwariya	C-DAC, Pune
18	Suresh V	C-DAC, Pune
19	Taruna Bhatia	CDAC Mohali
20	Tushar Atamaram Fegade	CDAC, Pune
21	Vijay Madan	TSDSI – Convener WP
22	Chandrakanta Rathore	TSDSI – Coordinator WP

tsdsi

India's Telecom SDO

Telecommunications Standards Development Society, India

Registered Office Address
C-DOT Campus, Mandi Road, Mehrauli,
New Delhi, India – 110030
www.tsdsi.in