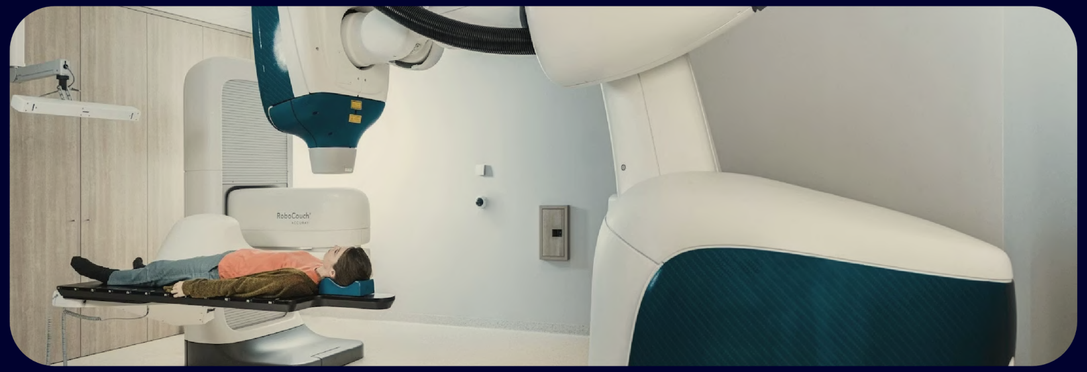


Enhancing Data Governance for Health Care Robots

About

Explores data management and governance strategies for health care robots, addressing challenges in ensuring data quality, privacy, and compliance while leveraging advanced technologies to improve patient care and operational efficiency.

AGENDA

Poor and Good Data Governance

Poor Governance in Healthcare Robotics: Key Challenges

Insufficient Internet Connectivity Planning

Reliance on Stable Connection: Federated learning systems require continuous network access.

Risk of Interrupted Updates: Outdated training parameters reduce robot efficacy.

Impact on Patient Care: Compromised care quality and potential harm to patients.

Limited Versatility of Robots

Narrow Task Design: Current robots address only specific, limited functions.

High Costs vs. Benefits: Significant investment without proportional returns.

Reduced Scalability: Minimal impact on broader healthcare needs.

Weak Access Control Policies

Incomplete Implementation: Access control measures remain at the planning stage.

Unauthorized Access: Increased risk of cyberattacks by both internal and external actors.

Data & Safety Risk: Breaches of sensitive medical data, compromising user safety.

Good Governance in Healthcare Robotics: Key Challenges

1

Federated Learning Framework

Localized Data: Sensitive data stays on individual devices, with only training parameters shared.

Reduced Breach Risk: Avoids centralizing data, minimizing exposure to cyber threats.

Collaborative Development: Enables teamwork among developers, researchers, and healthcare providers.

2

Adherence to GDPR and Consent Mechanisms

Informed Consent: Emphasis on obtaining clear participant permission for data collection and sharing.

Transparency: Open communication about data usage fosters user trust.

Data Quality: Secure and trusted processes encourage participants to share valuable insights.

3

Diverse User Data in Test Study

Inclusive Approach: Incorporates a broad range of participants, including elderly individuals.

Generalizability: Wider representation enhances model performance across different groups.

Acceptance: Increased usability and adoption of robotic solutions in varied healthcare settings.

GDPR Compliance in Healthcare Robotics

Ensuring GDPR compliance is critical in healthcare robotics to protect patient privacy, maintain data integrity, and build trust in the safety of emerging technologies

Challenges

Federated Learning Risk: Not entirely privacy-preserving, creating potential data leakage.

Incomplete Access Controls: Policies are only planned, risking unauthorized data access.

Article 5: Integrity and Confidentiality

Personal data must be processed ensuring data accuracy, consistency, and protection from unauthorized access or breaches.

Actions

- Encrypt Data: Secure information at rest and in transit.
- Utilize Differential Privacy: Add noise to training parameters to safeguard sensitive info.
- Regular Integrity Checks: Verify data accuracy and detect tampering.

Article 32: Security of Processing

Technical and organizational measures must protect personal data against breaches or unauthorized access.

Actions

- **Role-Based Access Controls (RBAC)**: Limit data access to authorized personnel only.
- **Blockchain Technology**: Establish transparent, tamper-proof logs of data access and modifications.
- **Regular ecurity Audits**: Identify and remediate vulnerabilities in the system.

MDR in Healthcare Robotics

Ensuring compliance with MDR standards is essential for the safe and reliable deployment of healthcare robots, maintaining patient well-being and regulatory approval.

Challenge

Compliance with MDR Standards: Robots must meet safety, risk management, and performance requirements.

Annex I: General Safety and Performance Requirements

Devices must be designed to ensure safety and performance for their intended use under normal conditions.

Actions:

- **Risk Assessments:** Identify potential hazards and implement mitigation strategies.
- **Robot Versatility:** Design robots capable of multiple tasks to enhance usability across diverse healthcare settings.
- **Real-World Testing:** Conduct rigorous trials in hospitals and home care environments for reliability and adaptability.

Ethical Principles

Participation

Patients should be consulted on how their health data is used in training models.

Equality and Non-Discrimination

Ensuring healthcare robots are trained on diverse datasets to avoid biases against underrepresented groups.

Data Privacy and Security

Using privacy-preserving technologies like differential privacy in federated learning models.

Accountability

Regular audits and accessible reporting mechanisms for patients to address concerns about data usage.

Transparency

Informing patients about how their data contributes to the functioning and improvement of healthcare robots.

Self-Identification

Ensures that patients feel empowered and respected when interacting with robots.

Tensions Among Ethical Principles

Privacy vs. Participation

Data Processing Details: Sharing information on how data is processed can compromise individual privacy.

Broader Exposure: Inviting patients to co-develop or provide feedback on healthcare robots may inadvertently reveal sensitive data.

Transparency vs. Security

Vulnerability Risks: Detailed disclosures of data processing can expose system weaknesses.

Algorithm Exploitation: Making robot algorithms public could invite malicious attacks, reducing overall safety.

Equality vs. Self-Identification

Unequal Representation: Allowing voluntary self-identification might leave out groups who opt not to share personal attributes.

Underrepresentation: Patients from marginalized communities may avoid disclosing sensitive information, resulting in biases in training data.

Synergies Among Ethical Principles

Privacy vs. Participation

Privacy Through Security: Strong encryption and strict access controls help prevent unauthorized data access, thus safeguarding privacy.

Federated Learning: Integrating differential privacy within federated learning models preserves patient confidentiality without compromising data utility.

Transparency & Accountability

Trust through Clarity: Providing clear, open information about data practices fosters user trust and supports responsible governance.

Patient Empowerment: Explaining how data is used in healthcare robotics promotes ethical compliance and ensures all parties know who is held accountable.

Participation & Accountability

Inclusive Governance: Engaging patients, healthcare providers, and regulators in decision-making cultivates shared responsibility and adherence to human rights values.

Ethical & Regulatory Alignment: By involving diverse stakeholders, healthcare robotics solutions can better meet both ethical standards and regulatory requirements.

Data Management in Health Care Robots

Collecting High-Quality Data from Sensors

- Robots must have high-precision sensors (e.g., lidar, depth cameras, thermal imaging) to collect comprehensive data about the environment and patient needs.
- Implement data pre-processing at the edge (on the robots) to filter irrelevant or noisy data before it is stored or used for training.

Ensuring Data Relevance

- Design algorithms to categorise and tag data based on its use case (e.g., mobility support, emotional interaction).
- Use supervised and unsupervised methods to ensure only relevant data is fed into federated learning models.

Managing Diverse Data Formats

- Develop a standardised data schema that supports interoperability across different environments (hospital systems and home networks).
- Employ middleware solutions to unify data formats before transferring them to storage or analysis pipelines.

Data Quality and Metadata

01 **Maintaining High Data Quality**

Conduct regular data validation to identify and correct errors in real-time, such as sensor malfunctions or transmission delays.

Use redundancy checks and error-detection codes to ensure data accuracy during transmission.

---

02 **Metadata Management**

Automate metadata generation to include details such as timestamps, sensor types, and locations at the time of data collection.

Implement a metadata registry to catalogue and retrieve information efficiently during training or troubleshooting.

---

03 **Overcoming Standardisation Challenges:**

Develop a centralised protocol for hospitals and home environments to adhere to data standards.

Provide templates and tools for partners (hospitals, vendors) to align their systems with these standards.

Real-Life Data Management Issues

Avoiding Data Duplication in Federated Learning

Implement deduplication mechanisms at the data collection and storage levels.

Track changes to the training model versions to prevent redundant updates across robots.

Ensuring Secure Data Exchange

Use encryption protocols (e.g., TLS, end-to-end encryption) during the transfer of federated learning parameters.

Deploy secure multi-party computation (MPC) or homomorphic encryption to protect sensitive data in shared computation.

Overcoming Connectivity Challenges

Enable offline capabilities for robots, where they store updates locally and sync once the connection is re-established.

Partner with telecom providers to explore affordable connectivity solutions in underserved areas.

Building a Robust Data Governance Framework

Defining Roles and Responsibilities

Appoint data stewards in both hospital and home environments to oversee data quality and compliance.

Assign accountability for specific areas, such as privacy (Data Protection Officers) and security (IT managers).

Establishing Clear Policies

Develop comprehensive guidelines for data lifecycle management, from collection to disposal.

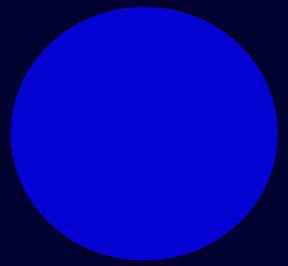
Ensure policies are compliant with GDPR and other relevant laws, specifying roles for handling breaches and incidents.

Continuous Monitoring and Audits

Use automated tools for logging data access and modifications to detect anomalies.

Conduct regular third-party audits to evaluate the effectiveness of governance measures.

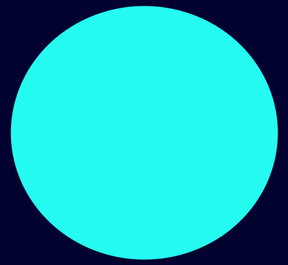
Addressing Social and Ethical Issues



Access Control Policies

Implement role-based access control (RBAC) to ensure only authorised personnel can access specific datasets.

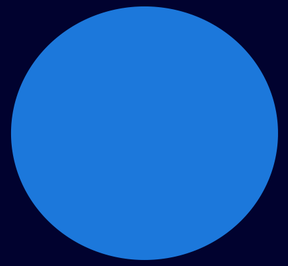
Introduce time-limited access for external researchers or engineers working on the robots.



Aligning Policies with Regulations

Engage legal experts during the design phase to ensure compliance with GDPR and medical data regulations.

Regularly update policies to align with evolving legal and ethical standards.



Gaining User Consent

Use clear, simple language in consent forms to inform users about how their data will be used.

Provide opt-in and opt-out mechanisms for data-sharing preferences.

“

Robots in healthcare need governance, or they might prescribe you Wi-Fi instead of medicine!

Practical Steps to Implement Governance

Starting with a Pilot Phase

Launch a small-scale implementation in hospitals, focusing on specific wards or use cases.

Use the pilot phase to identify and address technical and operational challenges before scaling.

Creating Feedback Loops

Regularly collect feedback from stakeholders, including patients, caregivers, and IT staff, to refine data governance practices.

Conduct focus groups and surveys to assess satisfaction with the robots' performance and data handling.

Training Staff

Develop training programs to educate hospital staff and caregivers on data privacy, security protocols, and governance policies.

Create easy-to-understand guides and provide ongoing support for managing robots and their data.

Thank you!