Data Governance in Health care robots

Suryalaxmi Ravianandan

Introduction to case study

- The case study focuses on healthcare robots as a solution to two critical issues:
  - Aging population
  - Shortage of care staff

  These problems are pressing in many societies, where the demand for caregiving is outpacing the availability of human caregivers.
- Robots like Grace, Moxi and Robear are being developed with advanced capabilities to fill these gaps.
  - Designs are task-specific, meaning they can only perform limited functions.
  - Complexity of their hardware and software adds to the challenges of general adoption, making them expensive and less accessible.
- Emerging Technologies
  - Advancements in **deep learning** and **sensor technology**—such as lidar, depth cameras, and thermal imaging—could revolutionize healthcare robotics.
  - **Federated learning** is a promising method that trains models across multiple robots while keeping data localized.

Introduction to case study

- Aim is to develop a **comprehensive data governance strategy**.

Key responsibilities include:

- ✓ Ensuring compliance with legal regulations.
- ✓ Addressing ethical concerns, such as data privacy, informed consent.
- ✓ Identifying social challenges, like access inequalities and trust-building among users.
- ✓ Integrating privacy-preserving technologies like federated learning to safeguard sensitive medical data.

I. Poor and Good Data Governance

Poor Data Governance.

	Issues	Risk	Consequences
Insufficient Internet Connectivity Planning	The federated learning system relies on stable internet connectivity, which may not be universally available.	Interrupted updates to training parameters can lead to outdated models, reducing robot efficacy.	Lower quality of care and potential harm to patients.
Limited Versatility of Robots	Current robots are designed for narrow tasks, failing to maximize their potential.	High costs without proportional benefits due to limited utility.	Reduced return on investment and limited scalability in healthcare systems.
Weak Access Control Policies	Access control policies are only planned, not fully implemented or detailed.	Unauthorized access by internal or external actors. Increased vulnerability to cyberattacks.	Breach of sensitive medical data and compromised user safety.

Good Data Governance

	Practice	Benefits	Impact
Federated Learning Framework	Sensitive data remains localized, with only training parameters shared.	Minimizes data centralization, reducing exposure to breaches.	Encourages collaboration among developers, researchers, and healthcare providers.
Adherence to GDPR and Consent Mechanisms	The project emphasizes obtaining participant consent for data collection and sharing.	Transparency in data usage builds trust among users.	Participants feel more secure in sharing data, improving the quality of collected insights.
Diverse User Data in Test Study	Inclusion of diverse participants, including elderly individuals, ensures comprehensive data collection.	Improves model generalizability for broader applications.	Enhanced usability and acceptance of robots across demographics.

II. Laws and Regulations and How They Affect Design

Laws and Regulations

1. General Data Protection Regulation (GDPR) Compliance

- **Issue:**
  a) The federated learning approach is not entirely privacy-preserving, creating risks of data leakage.
  b) Data sharing, even as training parameters, may still indirectly reveal sensitive information.
  c) Access control policies are only planned but not fully implemented, risking unauthorized data access.

- **Potential Non-Compliance:**
  a) Article 5: Processing personal data must ensure integrity and confidentiality.
  b) Article 7: Explicit and informed consent is required for data processing.
  c) Article 32: Mandates the implementation of technical and organizational measures to secure personal data.

Laws and Regulations

1. General Data Protection Regulation (GDPR) Compliance

- **Issue:**
  a) The federated learning approach is not entirely privacy-preserving, creating risks of data leakage.
  b) Data sharing, even as training parameters, may still indirectly reveal sensitive information.
  c) Access control policies are only planned but not fully implemented, risking unauthorized data access.

Article 5: Integrity and Confidentiality

Personal data must be processed in a way that ensures its integrity (accuracy and consistency) and confidentiality (protection from unauthorized access or breaches).

Actions:

- Implement **data encryption** during storage and transmission to prevent unauthorized access.
- Use **differential privacy** to add noise to training parameters, making it harder to infer sensitive information from shared data.
- Conduct regular **integrity checks** to ensure data accuracy and prevent tampering.

Laws and Regulations

1. General Data Protection Regulation (GDPR) Compliance

- **Issue:**
  a) The federated learning approach is not entirely privacy-preserving, creating risks of data leakage.
  b) Data sharing, even as training parameters, may still indirectly reveal sensitive information.
  c) Access control policies are only planned but not fully implemented, risking unauthorized data access.

Article 7: Explicit and Informed Consent

Data processing must have explicit, informed, and revocable consent from participants.

Actions:

- Develop **clear and accessible consent forms** that explain how data will be collected, used, and shared.
- Provide participants with the ability to **opt-in or opt-out** of specific data processing activities, such as participation in federated learning.
- Create a **mechanism for consent withdrawal** that allows users to revoke their consent at any time.

Laws and Regulations

1. General Data Protection Regulation (GDPR) Compliance

- **Issue:**
  a) The federated learning approach is not entirely privacy-preserving, creating risks of data leakage.
  b) Data sharing, even as training parameters, may still indirectly reveal sensitive information.
  c) Access control policies are only planned but not fully implemented, risking unauthorized data access.

Article 32: Security of Processing

Technical and organizational measures must be implemented to secure personal data against breaches or unauthorized access.

Actions:

- Enforce **role-based access controls (RBAC)** to restrict data access to authorized personnel only.
- Deploy **blockchain technology** for transparent and tamper-proof logging of data access and modifications.
- Conduct **regular security audits** to identify and address vulnerabilities in the system.

Laws and Regulations

2. Medical Device Regulations (MDR)

- **Issue:**
  a) The design of healthcare robots must comply with MDR standards for medical devices, including safety, risk management, and performance monitoring.
  b) Limited robot versatility could fail to meet the MDR's usability and reliability requirements.

- **Potential Non-Compliance:**
  a) Annex I: General safety and performance requirements.
  b) Article 10: Manufacturers must implement a quality management system.

Laws and Regulations

2. Medical Device Regulations (MDR)

- **Issue:**
  a) The design of healthcare robots must comply with MDR standards for medical devices, including safety, risk management, and performance monitoring.
  b) Limited robot versatility could fail to meet the MDR's usability and reliability 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**: Perform detailed evaluations to identify potential hazards and implement mitigation strategies.
- **Robot Versatility**: Design robots capable of performing multiple tasks to improve usability across diverse healthcare scenarios.
- **Test in Real-World Environments**: Conduct rigorous testing in both hospitals and home care settings to ensure reliability and adaptability.

Laws and Regulations

2. Medical Device Regulations (MDR)

- **Issue:**
  a) The design of healthcare robots must comply with MDR standards for medical devices, including safety, risk management, and performance monitoring.
  b) Limited robot versatility could fail to meet the MDR's usability and reliability requirements.

Article 10: Quality Management System

Manufacturers must implement a quality management system (QMS) to maintain compliance with MDR, including ongoing performance evaluations and documentation.

Actions:

- **Regular Performance Evaluations**: Monitor and document the robot's performance to identify areas for improvement and ensure ongoing compliance.
- **Post-Market Surveillance**: Implement systems to collect feedback and monitor the robots after deployment, ensuring continuous safety and reliability.
- **Documentation and Reporting**: Maintain detailed records of all processes, from risk management to performance evaluations, as required by MDR.

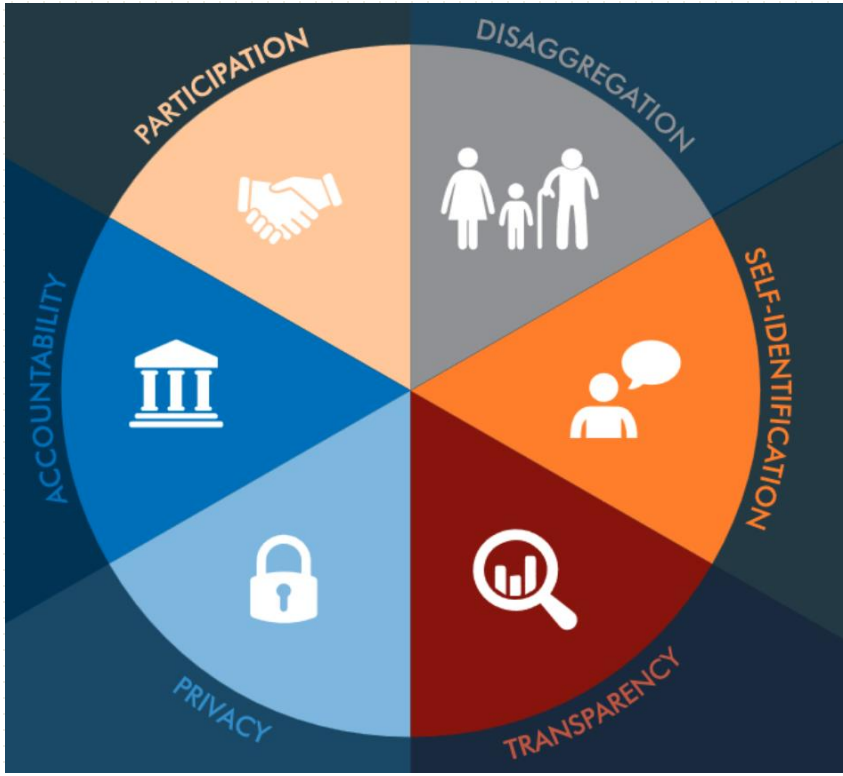
III. Ethical Considerations, Tensions Between Privacy, Fairness, and Security

Ethical Principles

Key Principles of HRBAD

- **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

Human Rights-based Approach to Data (HRBAD)



Tensions between Ethical Principles

Tension: The principles conflict with each other and restrict each other's effectiveness		
Privacy vs. Participation	Engaging individuals in the decision-making process about their data (participation) may require sharing detailed information about how their data is processed, which could unintentionally compromise privacy.	Involving patients in healthcare robotics development may expose their sensitive health data to broader discussions.
Transparency vs. Security	Providing detailed transparency about data processing could expose vulnerabilities, increasing security risks.	Disclosing the algorithms used in healthcare robots to ensure accountability might make them susceptible to malicious exploitation.
Equality vs. Self-Identification	Enabling voluntary self-identification may lead to unequal representation if certain groups opt not to disclose key attributes.	Patients from marginalized groups may avoid identifying their ethnicity, resulting in underrepresentation in the training data for healthcare robots.

Synergies between Ethical Principles

Synergy: Operationalizing one principle helps successful implementation of the other principle		
Privacy and Security	Strong security measures, such as encryption and access controls, also enhance privacy by preventing unauthorized data access.	Federated learning with differential privacy protects patient data while maintaining confidentiality.
Transparency and Accountability	Transparent data practices build trust and facilitate accountability, ensuring that stakeholders understand how data is used and who is responsible.	Providing patients with clear explanations of data use in healthcare robotics increases trust and fosters ethical compliance.
Participation and Accountability	Engaging stakeholders in data governance fosters accountability, ensuring decisions align with human rights principles.	Involving patients, healthcare providers, and regulators in decision-making ensures that healthcare robots meet ethical and regulatory standards.

Thank you…