Decentralized, Secure and Privacy-Preserving Sharing of Health Data

Noshaba Naeem
PhD Research Scholar
Department of Science and Industry Systems
University of South-Eastern Norway (USN), Campus Kongsberg
October 31, 2025
Email: noshaba.naeem@usn.no

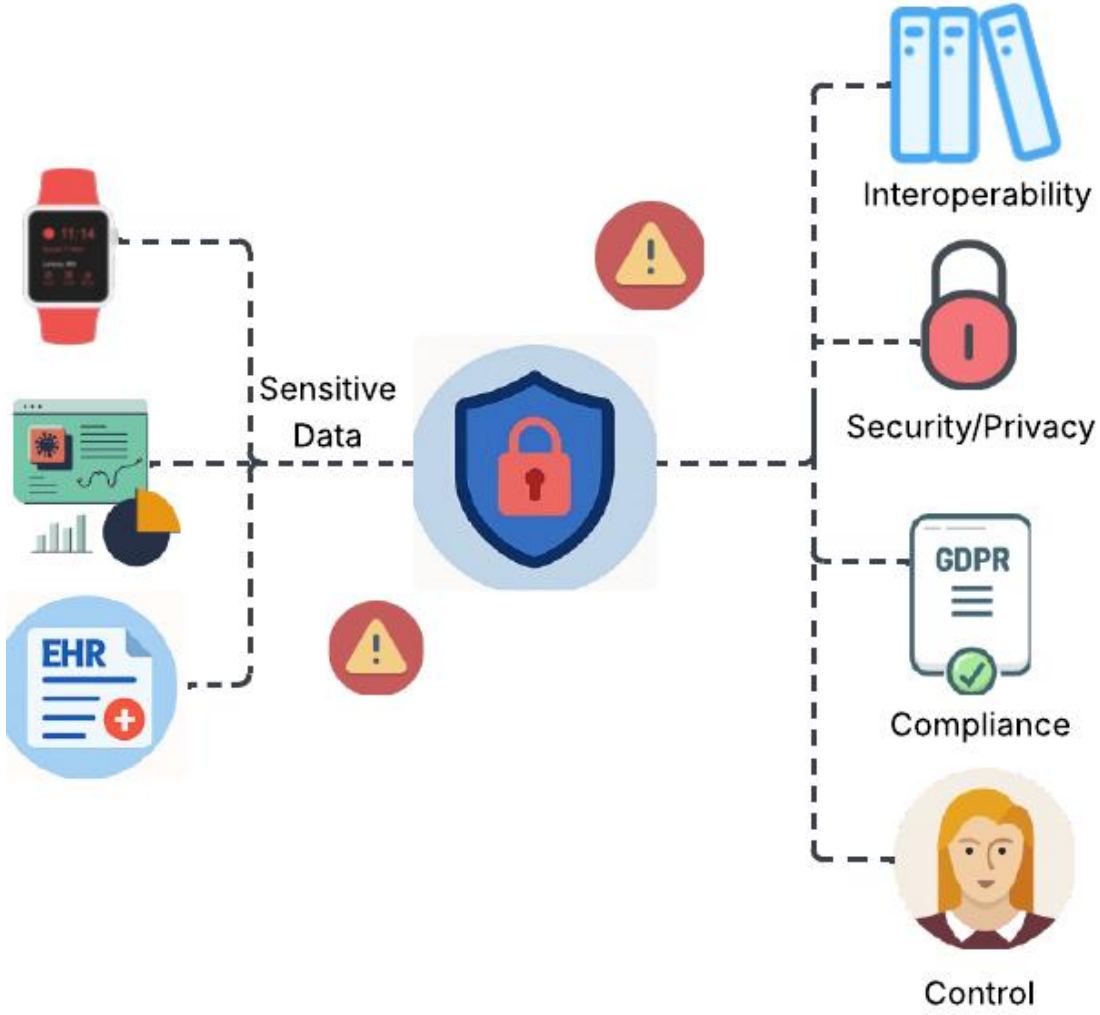
Universitetet i Sørøst-Norge

Problem with Centralized Systems

Traditional systems use centralized architectures

- Opaque Governance
- Single point of failure
- Data breaches
- Patients lose control once data is shared

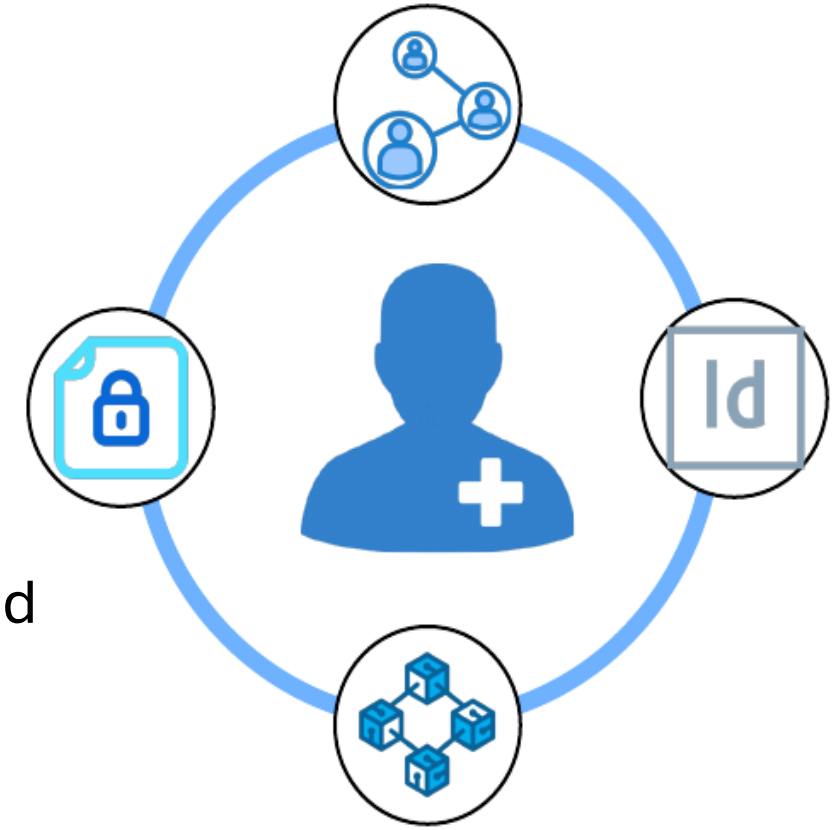
Requirement of sovereignty, control, and trust



Centralized systems are struggling to deliver both

Why Decentralization Matters

- Healthcare data is increasingly digital and highly sensitive.
- Regulations demand transparency and user control.
- Cross-border data sharing remains difficult .
- Healthcare transformation depends on secure, trusted data exchange.



What Decentralization Provides

- Decentralization distributes control across multiple trusted organizations.
  - Reduces dependency on one authority and improves resilience.
- Decentralization alone DOES NOT ensure privacy or security.
- Requires Privacy-Enhancing Technologies (PETs) to enforce privacy cryptographically.

Privacy-Preserving & Cryptographic Techniques

- **Zero-Knowledge Proofs (ZKP):** Prove statements without revealing data.
  - selective disclosure
- **Proxy Re-encryption:** Allows a semi-trusted proxy to transform ciphertexts from one key to another.
  - Supports secure delegation and access revocation.
- **Differential Privacy:** Adds noise to preserve anonymity in aggregated data.
  - Anonymity
- **Attribute-Based Encryption (ABE):** Encrypt data so only recipients with specific attributes can decrypt.
  - Fine-grained, policy-based access control
- **Homomorphic Encryption (HE):** Enables computations on encrypted data.
  - secure cloud analytics

Challenges

- Difficult to enforce consent and dynamic access policies across multiple nodes.
  - Systems must decide who, for how long, and what data fields
- Integrating advanced encryption in real-time healthcare systems
- Errors can expose sensitive data or block care
- Instant revocation across the network without re-encryption (Propagation delays, Key management overhead, Consistency)
- Balancing security, usability, and compliance remains unsolved.

Research Goal

Decentralized and privacy-preserving health data sharing framework

- Patient-controlled access to encrypted electronic health records.
  - Fine-grained access control and verifiable authorization mechanisms.
  - Access delegation.
- Timely and system-wide revocation of access rights.
  - Synchronized key rotation or proxy re-encryption protocols.
- All actions remain GDPR and EHDS compliant.
  - Auditable consent management and privacy-preserving data processing.

Broader Impact

- Restores trust in digital health systems through verifiable privacy, not promises.
- Enables secure cross-border healthcare collaboration
  - speeds up innovation in medical research and public health.
- Reduces manual key and access management.
- Supports future privacy-preserving infrastructures.

Thank You..!

Any Questions?