



FHI

*Fully Homomorphic Encryption for
Advanced Life-saving Technology and Healthcare*

<https://a4gq6-oaaaa-aaaab-qaa4q-cai.raw.ic0.app/?id=2arwf-lyaaa-aaaam-adila-cai>

AI, GameFi, SocialFi & NFTs

TRACK 2:

AI-POWERED SMART CONTRACTS



PRIVACY-PRESERVING MEDICAL DATA PLATFORM




TO ENSURE SENSITIVE HEALTHCARE DATA CAN BE SECURELY PROCESSED WITHOUT EVER BEING DECRYPTED. THE PLATFORM ENABLES SECURE MEDICAL RECORDS STORAGE, ANALYSIS, AND SHARING BETWEEN PATIENTS, DOCTORS, AND HEALTHCARE PROVIDERS WHILE ENSURING DATA PRIVACY.



THE CORE FEATURE OF FHEALTH IS ITS ABILITY TO PERFORM COMPUTATIONS (SUCH AS ANALYTICS AND AI-BASED PREDICTIONS) DIRECTLY ON ENCRYPTED DATA USING FHE, WITHOUT COMPROMISING USER PRIVACY.



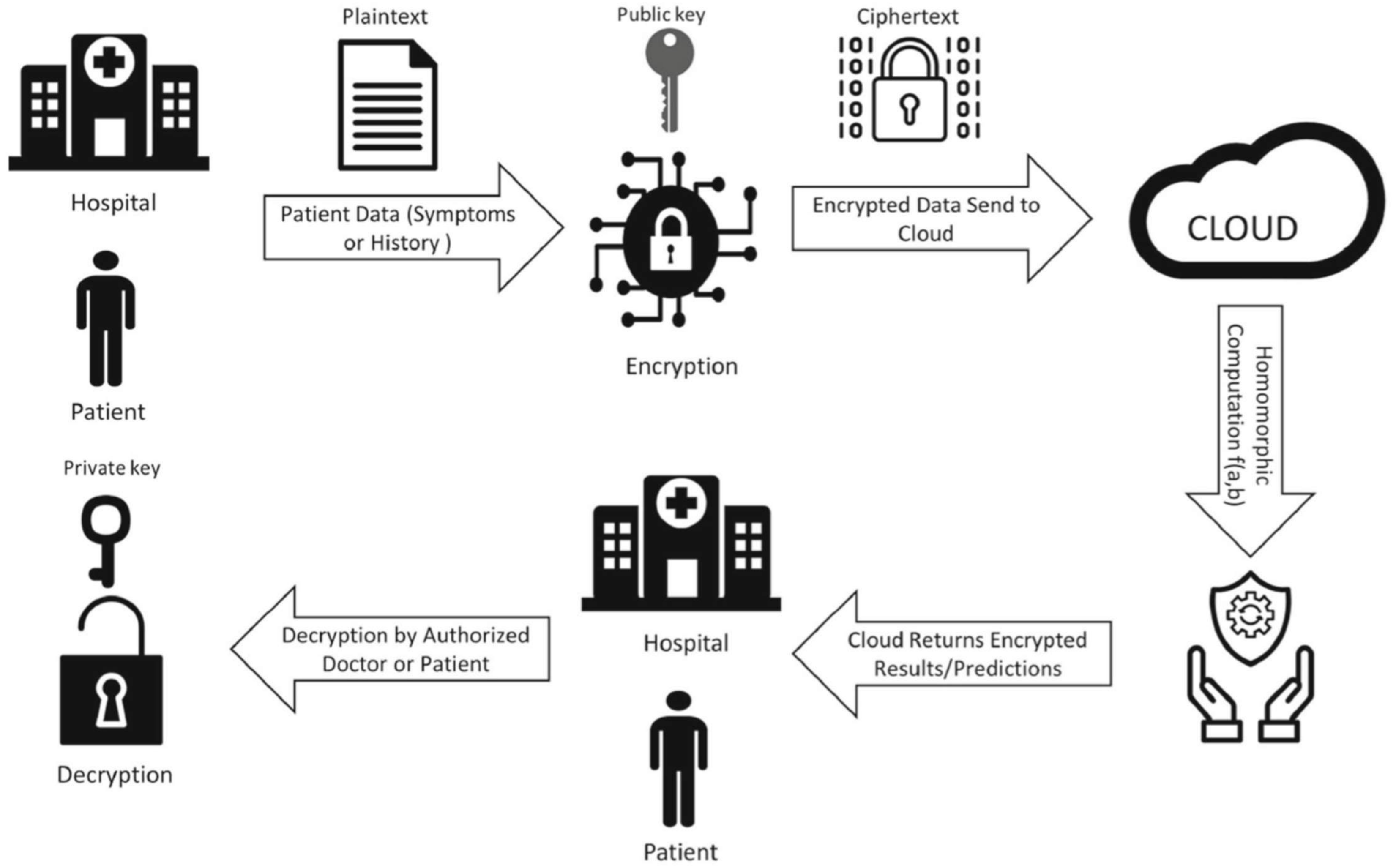
QUALITY
SERVICE



Fully Homomorphic Encryption

BUILT ON THE INTERNET COMPUTER (ICP) THAT LEVERAGES FULLY HOMOMORPHIC ENCRYPTION (FHE) GLOBAL ACCESSIBILITY TO SECURE HEALTHCARE SERVICES, ENSURING THAT PRIVACY-PRESERVING TECHNOLOGY BECOMES A STANDARD FOR HEALTHCARE WORLDWIDE.

BY BRINGING PRIVACY-PRESERVING TECHNOLOGY TO HEALTHCARE, FHEALTH AIMS TO REDEFINE TRUST BETWEEN PATIENTS, HEALTHCARE PROVIDERS, AND TECHNOLOGY. WE BELIEVE THAT IN THE FUTURE, SECURITY AND PRIVACY SHOULD NOT BE A CHOICE—THEY SHOULD BE BUILT INTO EVERY INTERACTION WITH HEALTH DATA.



Vision for FHEalth:

THE VISION OF FHEALTH IS TO REVOLUTIONIZE THE WAY HEALTHCARE DATA IS HANDLED BY CREATING A PRIVACY-FIRST, SECURE PLATFORM THAT EMPOWERS PATIENTS TO HAVE FULL CONTROL OVER THEIR SENSITIVE MEDICAL INFORMATION. BY LEVERAGING THE POWER OF FULLY HOMOMORPHIC ENCRYPTION (FHE) AND THE INTERNET COMPUTER (ICP), WE AIM TO ENSURE THAT MEDICAL DATA CAN BE SECURELY STORED, SHARED, AND ANALYZED WITHOUT EVER BEING EXPOSED, EVEN DURING COMPUTATION.





Features and Functionality:

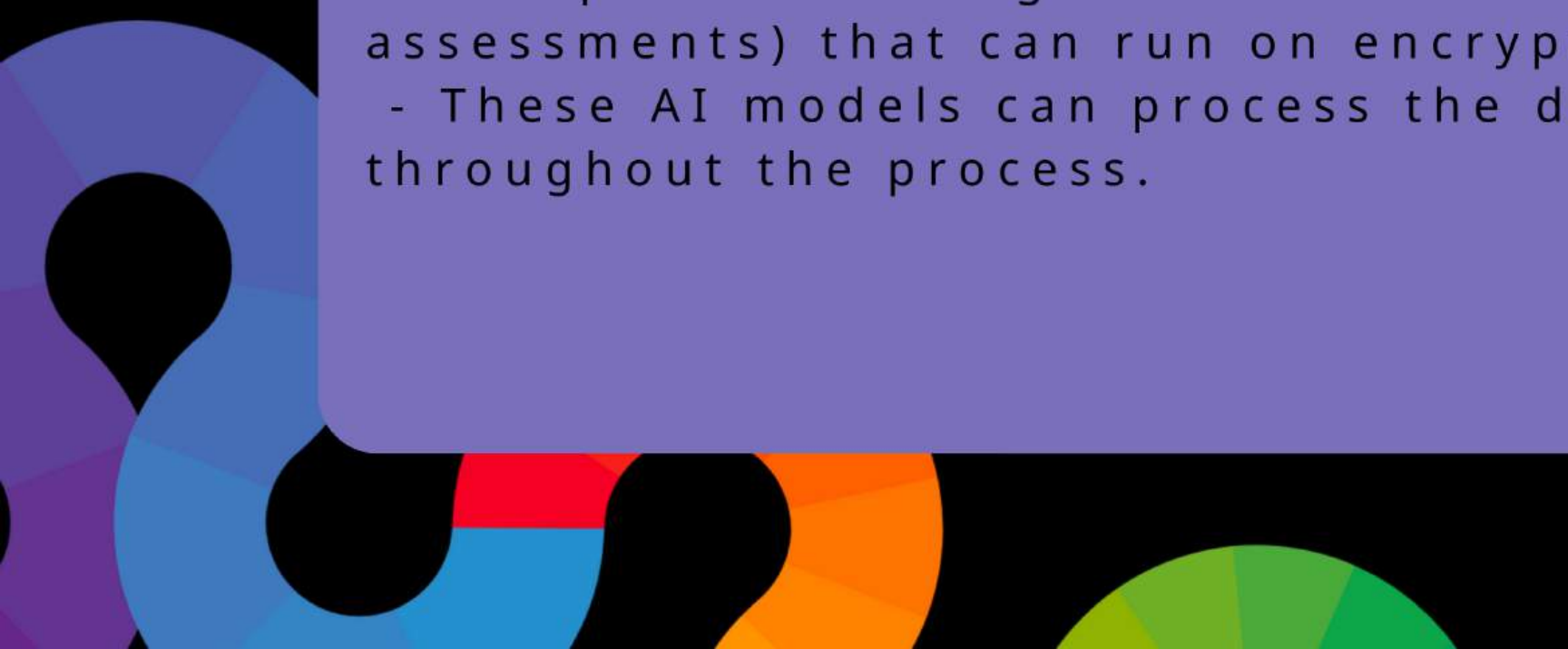
1. Privacy-Preserving Computation:

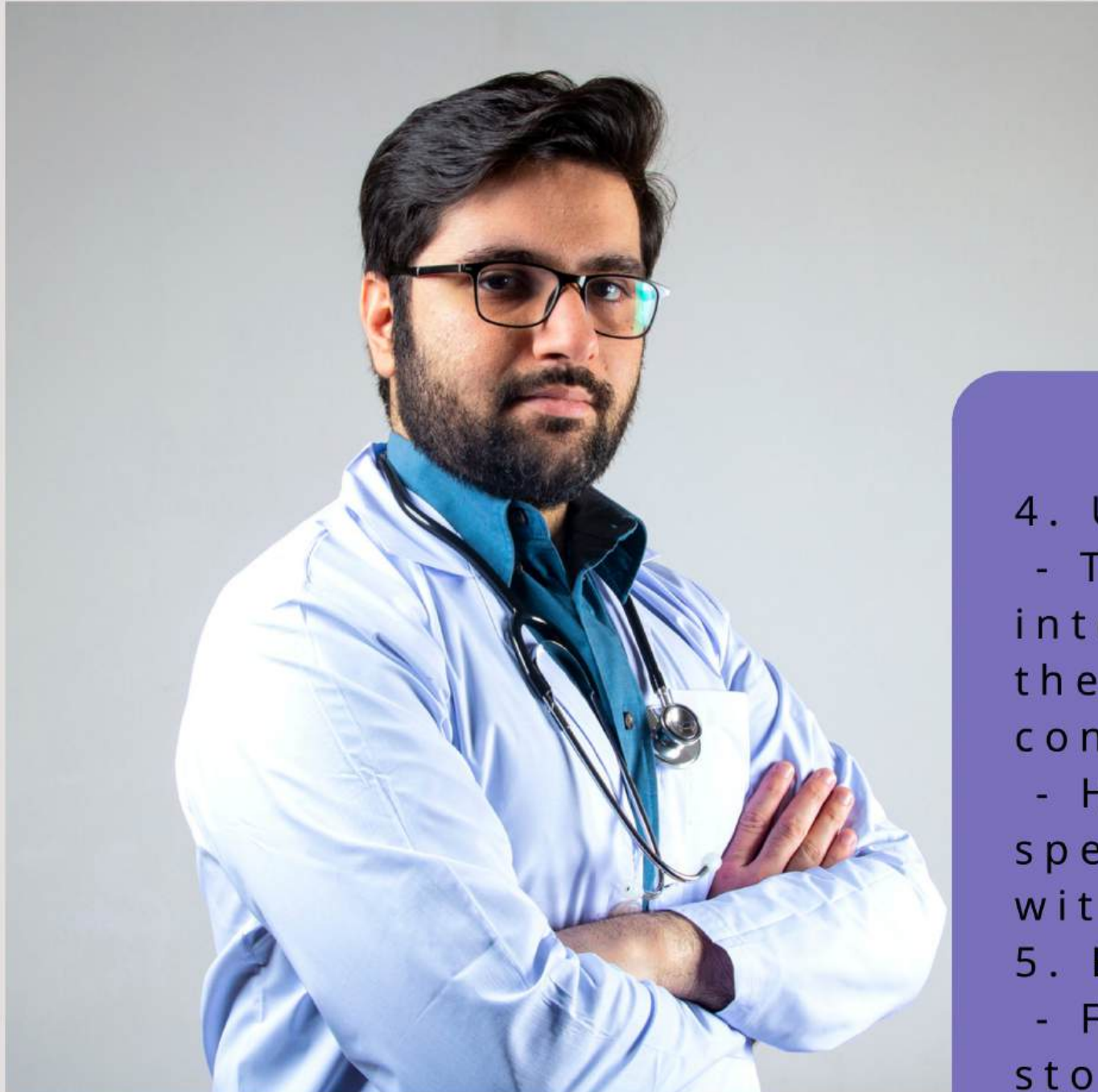
- FHEalth enables processing of encrypted health data, such as lab results, medical images, or prescriptions, directly on ICP canisters without exposing the data to third parties.
- The platform uses FHE to ensure that even during computations (like analytics or machine learning models), data remains encrypted.

2. Secure Medical Records Storage:

- Patient records are stored in ICP canisters in encrypted form, with no direct access to plaintext data by anyone except the authorized user.
- Patients and healthcare providers can securely share encrypted medical data through the platform, while the system ensures privacy at every stage.

3. AI-Assisted Health Analytics:

- The platform integrates AI models for medical analysis (e.g., disease prediction, risk assessments) that can run on encrypted data using FHE.
 - These AI models can process the data while it remains encrypted, ensuring privacy throughout the process.
- 



Take Care Of Your Health

4. User-Friendly Interface:

- The platform offers a simple and intuitive user interface, where patients can upload, view, and share their medical data with providers while maintaining full control over encryption keys.
- Healthcare providers can securely request access to specific data, and patients can grant permissions without ever exposing their raw data.

5. End-to-End Encryption:

- FHealth ensures that all data interactions, including storage, transmission, and computation, are encrypted end-to-end.
- Data is encrypted client-side and remains encrypted during computation within ICP canisters, with the decryption only happening on the client's device.

FHEalth envisions a future where:

PATIENTS ARE IN CONTROL OF THEIR DATA,
WITH THE ASSURANCE THAT THEIR PERSONAL
HEALTH INFORMATION IS ALWAYS PROTECTED,
NO MATTER HOW OR WHERE IT'S PROCESSED.
HEALTHCARE PROVIDERS CAN ACCESS THE
INSIGHTS THEY NEED THROUGH SECURE
COMPUTATIONS AND AI-DRIVEN ANALYTICS,
WITHOUT COMPROMISING PATIENT PRIVACY.
INNOVATIVE AI MODELS CAN TRANSFORM THE
HEALTHCARE INDUSTRY, OFFERING PREDICTIVE
AND PERSONALIZED MEDICAL INSIGHTS WHILE
MAINTAINING THE HIGHEST STANDARDS OF
DATA





Milestones



Milestones:

Milestone 1: Initial Platform Development (Weeks 1-3)

- Objective: Set up the foundation for the FHealth platform, including basic infrastructure for secure data handling.
- Deliverables:
 - Development of core ICP canisters that will handle encrypted data storage and transmission.
 - Basic user interface allowing users to upload encrypted health data.
 - Implementation of client-side encryption and decryption functionalities using an FHE library (e.g., Microsoft SEAL or HELib).

Milestone 2: FHE Integration and Encrypted Computation (Weeks 4-6)

- Objective: Integrate Fully Homomorphic Encryption into the platform and enable encrypted computations within the ICP canisters.
- Deliverables:
 - Implementation of encrypted data processing functions, allowing computations (e.g., addition, multiplication) on ciphertext data.
 - Initial deployment of AI models (e.g., for medical analytics) on the encrypted data stored within canisters.
 - Encryption of the computation results, which will be sent back to the user for decryption.

Milestone 3: Secure Medical Data Sharing (Weeks 7-9)

- Objective: Enable secure data sharing between patients and healthcare providers using FHE on ICP.
- Deliverables:
 - Feature allowing patients to share encrypted medical records with healthcare providers securely through ICP.
 - Implementation of role-based access control (RBAC), where patients can grant limited access to specific encrypted data.
 - Automated key management for users, ensuring easy access and sharing of encryption keys between authorized parties.



Milestones



Milestone 4: AI-Assisted Health Analytics on Encrypted Data (Weeks 10-12)

- Objective: Implement AI models for health analytics that operate directly on encrypted medical data.
- Deliverables:
 - Deployment of trained AI models (e.g., for disease prediction or patient risk scoring) that can perform analytics on encrypted patient data.
 - Optimization of FHE-based AI computation for efficiency, minimizing computational overhead and latency.
 - Testing and validation of AI results, ensuring the accuracy of the model's predictions post-decryption.

Milestone 5: User Testing, Security Audits, and Optimization (Weeks 13-15)

- Objective: Conduct user testing and third-party security audits to ensure the platform's robustness, security, and usability.
- Deliverables:
 - Completion of user acceptance testing (UAT) with a small group of patients and healthcare providers to gather feedback.
 - Independent security audit of FHE implementation to ensure no vulnerabilities exist in data encryption, computation, or sharing.
 - Optimizations to UI/UX and canister performance based on user feedback and audit findings.

Milestone 6: Full Platform Launch (Weeks 16-18)

- Objective: Launch the FHEalth platform to the public, ensuring full functionality and privacy-preserving features.
- Deliverables:
 - Public release of the platform with all features, including secure data sharing, encrypted computations, and AI-assisted analytics.
 - Final deployment on ICP with documentation and support for users and healthcare providers.
 - Marketing and outreach campaign targeting healthcare institutions and privacy-conscious users.

Get In Touch With Us

FHEALTH IS A SECURE, PRIVACY-PRESERVING HEALTHCARE PLATFORM THAT LEVERAGES THE ADVANCED CAPABILITIES OF FULLY HOMOMORPHIC ENCRYPTION AND THE DECENTRALIZED NATURE OF THE INTERNET COMPUTER (ICP) TO ENSURE THAT SENSITIVE MEDICAL DATA CAN BE STORED, SHARED, AND PROCESSED SECURELY. BY ENABLING ENCRYPTED AI COMPUTATIONS, IT PROVIDES CUTTING-EDGE ANALYTICS WHILE ENSURING THAT PATIENT PRIVACY IS NEVER COMPROMISED.





Thank you

