T1D REGISTRY - TECHNICAL ARCHITECTURE AND HOSTING REQUIREMENTS

T1D TECHNICAL ARCHITECTURE

In defining the architecture of the solution, we prioritize data interoperability as a core element. Data interoperability is crucial for the seamless exchange, understanding, and effective utilization of health information across diverse systems. Our approach involves creating an interoperable data ecosystem that facilitates the smooth flow of health data, enabling national programs and policymakers to access and utilize information for analysis, policy decision-making, and overall improvement of outcomes.

At Dure, we have developed various applications and interoperability layers for multiple solutions, leveraging the principles of HL7 FHIR. Our expertise extends to the development and implementation of FHIR servers to meet diverse data exchange needs. This interoperable data ecosystem consolidates multiple data systems under one umbrella, creating a centralized platform. Developed using open- source technologies, this platform is fully owned and managed by the country.

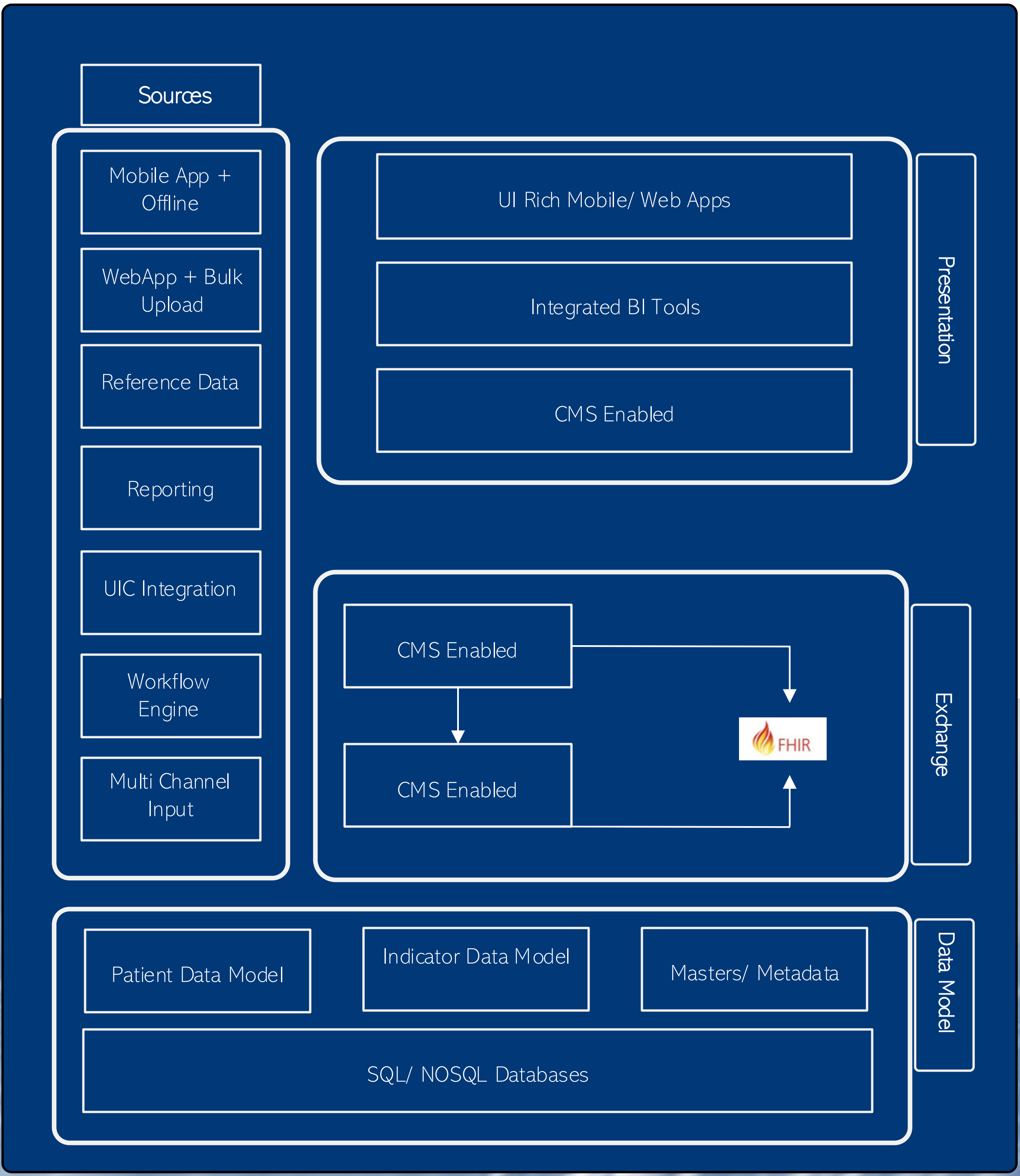
Importantly, our solution seamlessly integrates with existing data systems, avoiding duplication of efforts and maximizing efficiency.

As part of building the interoperability layer, we propose establishing a health information exchange as the backbone, facilitating data exchange using standards such as HL7 FHIR.

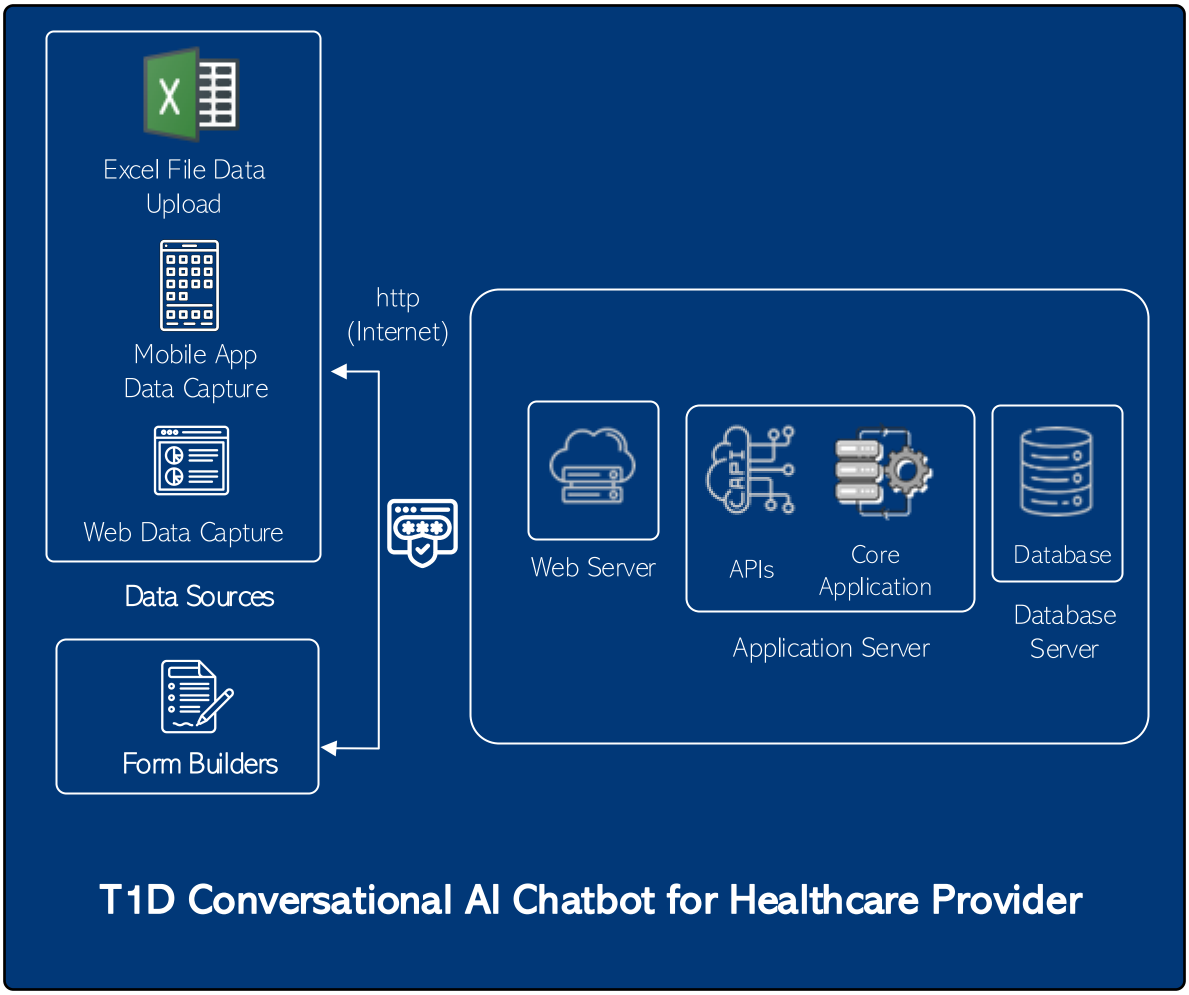
This architecture supports the exchange of case-based and aggregated data over a FHIR data layer, with centralized master data management. The integrated solution enables existing systems, including DHIS2, CLM, routine data, and other applications, to send and receive data through a central exchange.

Establishing a central terminology, registry, and metadata library, along with a unique patient identification system, enhances interoperability between systems. A centralized database acts as a repository for patient data from various sources, providing program managers with real-time, unified access.

T1D TECHNICAL ARCHITECTURE



SERVER SIZING FOR CDIC INITIATIVE



(1) WEB SERVER

- VM CPU: 4 Core
- RAM: 16 GB HDD:
- 250 GB OS: Linux
-

(1) APP SERVER

- VM CPU: 8 Core
- RAM: 64 GB HDD:
- 500 GB OS: Linux
-

(1) DB SERVER

- VM CPU: 4 Core RAM: 32
- GB HDD: 250 GB OS:
- Linux – Postgresql

DAILY BACKUP / DR

- Azure ASR – Another compliant data centre
- BlobStorage for local images

HOSTING AND DEPLOYMENT STANDARDS

The open-source solution adheres to rigorous hosting and deployment standards, ensuring both reliability and compliance with local regulations. The deployment process is designed to be flexible, accommodating a range of hosting options while prioritizing data sovereignty and compliance with local laws. Network can choose between cloud-based deployment or on-premises hosting, allowing them to tailor the solution to their specific needs and preferences.

For cloud-based deployment, the solution is compatible with major cloud service providers, facilitating a smooth and scalable implementation. It leverages industry-standard encryption protocols to safeguard data during transmission and at rest. Additionally, the cloud deployment model enables automatic updates and patches, ensuring the latest security measures are consistently applied.

The data centre of the cloud will be within the country and in compliance with local laws.

The option for on-premises deployment offers complete control over their infrastructure, vital for compliance with data residency requirements and privacy regulations. The solution provides detailed deployment documentation to guide organizations through the installation process, emphasizing best practices for secure and compliant deployment on their own servers.

To address the intricacies of compliance, the solution actively monitors changes in data protection laws and updates its features accordingly. Regular software updates include enhancements to meet evolving compliance standards, ensuring that the deployed solution remains aligned with the latest legal requirements.

DATA SECURITY

The solution’s data security measures contribute to a robust and holistic approach, safeguarding the integrity and confidentiality of the information managed by the solution. By integrating these security features, the solution not only protects sensitive data but also shares security awareness and responsibility among its users.

Data Ownership:

Data ownership is a fundamental aspect of the solution's data security framework. The system clearly defines data ownership, establishing accountability for the information within the network. Access to data is carefully controlled, ensuring that only authorized individuals or entities have the designated ownership rights. This helps maintain a clear and structured data governance model, contributing to transparency and accountability in data handling practices.

Data Encryption:

To enable data security, the solution implements robust encryption mechanisms. Data is encrypted both at rest within the storage infrastructure and during transit between the server and user devices. This safeguards sensitive information from unauthorized access or interception, reinforcing the confidentiality of the data and complying with industry best practices for securing digital assets.

Data Access Control:

Granular control over data access is a key feature of the solution's security architecture. Access permissions are granted based on predefined roles and responsibilities. Users are assigned specific roles, dictating the level of access they have to different types of data. This ensures that individuals can only interact with the data relevant to their functions, reducing the risk of unauthorized access or unintended data modifications.

DATA SECURITY

Multi-Factor Authentication (MFA):

To reinforce user authentication and prevent unauthorized access, the solution incorporates Multi-Factor Authentication (MFA). This additional layer of security requires users to verify their identity through multiple authentication factors, such as passwords, biometrics, or one-time codes. MFA enhances access control, adding an extra level of defense against potential security threats like unauthorized logins or data breaches.

Audit Trails:

Maintaining detailed audit trails is essential for monitoring and analyzing data-related activities within the solution. The system keeps comprehensive logs that record data access and any changes made to the information. These audit trails serve as a crucial tool for security investigations, compliance audits, and tracking user activity. They contribute to accountability and transparency in the use of sensitive data.

Data Protocols:

The solution establishes and enforces rigorous data security protocols. These protocols define the rules and guidelines for how data should be handled, processed, and shared. By adhering to these protocols, the solution ensures a consistent and secure approach to data management, aligning with industry standards and regulatory requirements.

Security Training:

A proactive approach to security is embedded in the solution's design. Security training is integrated into the user onboarding process, ensuring that individuals are well-informed about best practices and security measures. This training empowers end users to make informed decisions and reduces the likelihood of security incidents resulting from unintentional actions.

T1D Registry - Technical architecture and hosting requirements

T1D/2024/

Photo credits
©Pexels