PHILIPS

HealthSuite

digital platform

Store

Our service to acquire, manage and archive consumer and clinical data from applications and devices through secure cloud-hosted repositories.

Store offers a range of storage services to match data types and the requirements of customer applications. The services acquire, store and archive data in different types of cloud-hosted repositories.

Value

- **Managed service:** Use a host of features and advantages that come with a managed service, rather than a raw brokered service
- **Collect and store data**: Data from users, health and wellness devices, and clinical datastores across the health eco-system in a managed cloud repository
- **Open APIs**: Facilitate access to health data from multiple sources (devices, applications, systems) and enable faster development of consumer and professional applications
- **Data Security**: Secure and encrypted storage capabilities, access control and healthcare compliant auditing and logging all enhance the privacy and security of personal and clinical data

Clinical Data Repository Features

(FHIR Server)

The Clinical Data Repository (CDR) consists of CDR is a scalable implementation of the Fast Healthcare Interoperability Resources (FHIR) specification and associated services to aggregate data and enable authorized users to access and share data appropriate for their roles.

- **Data aggregation**. The CDR is a standard FHIR-based repository that provides a highly structured operational, rather than analytical, data store to support care delivery. The CDR aggregates data from users and clinical systems to create a longitudinal patient record.
- **Multi-Tenancy**. The CDR is designed as a multi-tenant data repository. Data from different organizations is stored separately in different instances
- **Standardized APIs**: are provided by the CDR. The CDR uses the open FHIR standard to provide REST APIs for standardized data access and representation of clinical data. It supports Create, Read, Update and Soft Delete operations on FHIR resources out- of-the-box, with a Hard Delete capability to support EU General Data Protection Regulations
- **Access control** leverages Authorize - Identity and Access Management services to provide Organization-based Access Control in which Administrators specify which users (individuals or organizations) may access an individual's health record, what they can access, and which operations they can perform. It also allows consumer and healthcare provider users to register with HSDP, so that they can start consuming the FHIR API provided by the CDR
- **Integrated auditing and logging** integrates Host – Auditing and Logging to provide auditing and logging of events on the CDR
- **Encryption**: The CDR encrypts data at rest and in transit

Telemetry Data Repository Features

The Telemetry Data Repository (TDR) is a service for storing user data and observations, as well as device data. Since it is optimized for speed, throughput, reliability and scalability, it is well suited to be an operational repository for clinical- and health applications for (near) real time writes and reads of structured and unstructured health-, observation-, and device data.

- **Data storage and retrieval** of small, high-velocity (semi) structured data resources, with size < 500KB is the primary intent of the TDR, with support for storage and retrieval of larger data items (JSON or binary blob) with lower performance. Search capabilities retrieve observations based on key, time-series, or other meta data
- **Multi-Tenancy** is supported by the TDR, which is designed as a multi-tenant data repository. Separate instances of the TDR are available clients based on regulatory/customer requirements
- **Contract management** for the TDR enables flexible, customer-defined structure of the data
- **Standardized APIs** are provided by the TDR. The REST APIs are available to retrieve the data with a key or query condition, can index the whole payload for search purposes and support Create, Read, Update and Delete operations. Security, privacy, and access control consists of Authorize-based identities and scope-based access control with configurable field-level encryption
- **Integrated auditing and logging** is enabled by integrating Host Auditing and Logging to provide auditing and logging of events
- **Encryption** is provided to ensure data security. The CDR encrypts data at rest and in transit

S3 Credentials Service Features

Store – S3 Credentials Service provides the ability to integrate the Authorize Identity and Access Management service directly to S3 storage for uploading and downloading data.

- The **core functionality** for the Credentials service is to define access permissions for users, generate temporary credentials for access to data, and provide direct access to S3
- **APIs for Administrators** to manage access control allow Administrators to define policies for users and groups, allowing access to S3 buckets and folders
- **APIs for clients** needing simple and direct access to S3 buckets are also available using the temporary credentials obtained from the Credentials Service

Consult hsdp.io for details