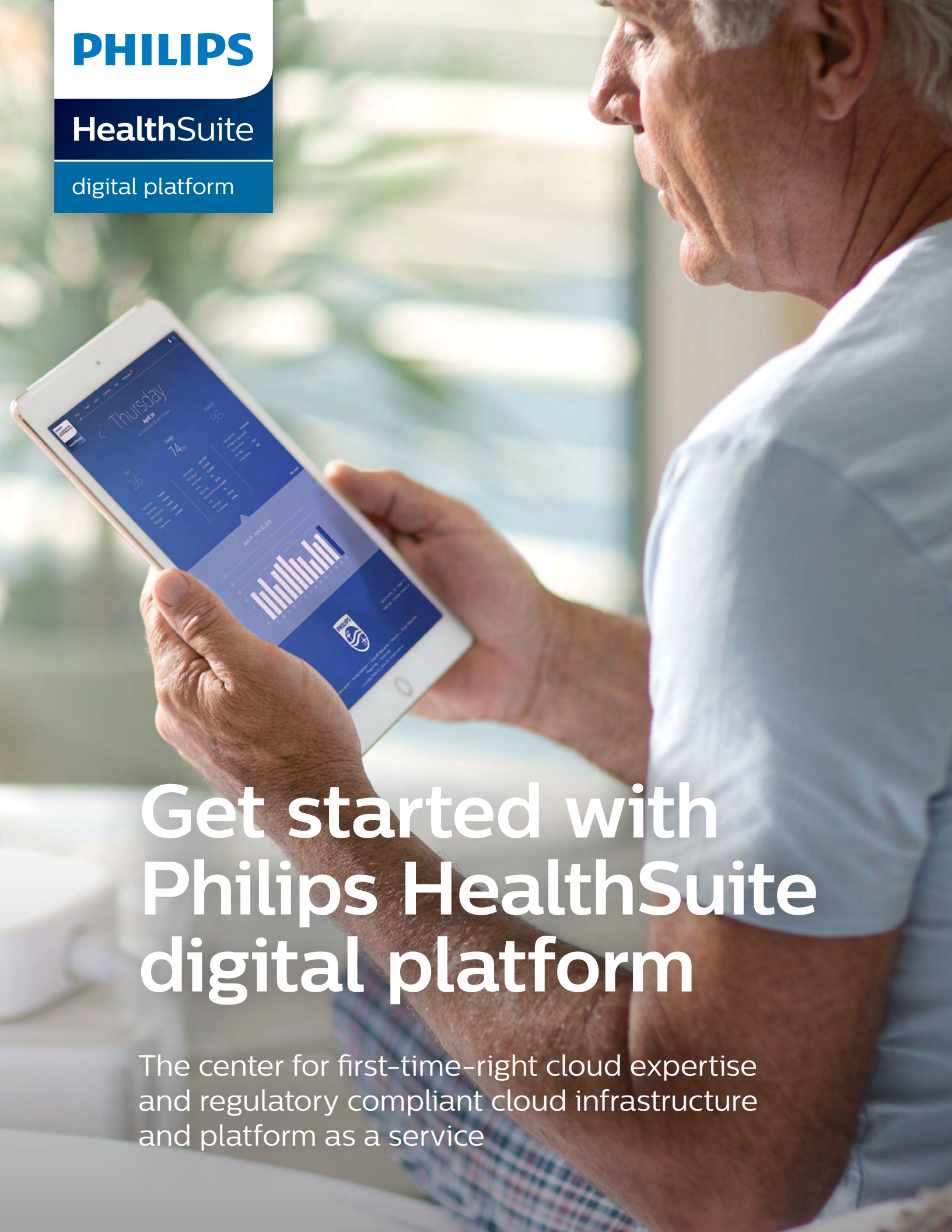
PHILIPS

HealthSuite

digital platform



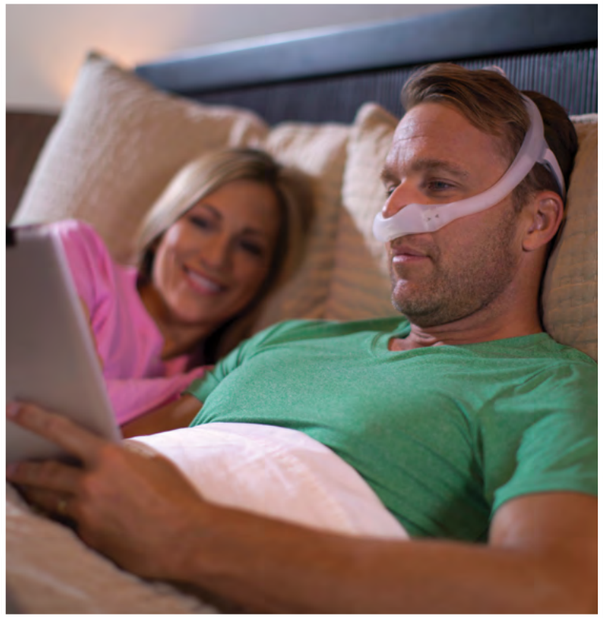
Get started with Philips HealthSuite digital platform

The center for first-time-right cloud expertise and regulatory compliant cloud infrastructure and platform as a service

Philips HealthSuite digital platform gives Philips and its partners the cloud expertise and capabilities to connect devices, collect electronic health data, aggregate and store data securely, analyze data and create solutions on the cloud.

This makes it possible to break down data silos and facilitate the innovation required to achieve seamless, connected and collaborative care that fulfills the 4 Ps of Digital Health: Precise, Personal, Predictive and Proactive.

Contents



PHILIPS
DoseAware
live review
Dr. van de Ven
Dr. Stas
Dr. Peeters
Dr. Kaufholz
Dr. Zuurmae
Dr. Lopez
Dr. Kremers
Dr. Duret
PHILIPS

What is HealthSuite digital platform?

Philips HealthSuite digital platform provides key components to enable the development of cloud-based consumer and healthcare solutions. It removes the burden of risk, cost, and resources so you can focus on developing and ensuring compliance of your value-added solutions.

Privacy, security and regulatory compliance: Information Security Management System, privacy, security and regulatory controls and operational security to ensure that the cloud infrastructure and platform as a service offering are compliant with appropriate privacy, security and regulatory requirements.

- Privacy, security and regulatory controls
- Operational security
- Penetration testing, other privacy and security testing and reviews
- Internal and external audits of compliance with privacy, security and regulatory controls to assure continuous improvement
- Security and privacy incident management and specialized security services, including Enforced Security Logging and containerization
- An extensive set of external compliance certifications and attestations to provide objective evidence of compliance to security and privacy regulations such as ISO 27001/18, SOC2, and HITRUST
- An Information Security Management system implemented by HSDP to ensure that services provided by HSDP are fully compliant with current level of certification
- A Quality Management System put in place by HSDP to ensure that HSDP meets the regulatory requirements of a Medical Device Data System (MDDS)
- A shared responsibility matrix provided by HSDP to ensure transparency of application owned compliance and to outline the steps required to ensure end-to-end compliance

Orchestrated cloud Infrastructure and platform as a service Managed cloud infrastructure and specialized platform services in regulatory compliant environment to address the needs of healthcare and consumer solution development.

- Customized, orchestrated platform services with APIs to address the needs of healthcare and consumer solution development
- Orchestration capabilities so dependent services work together seamlessly with HSDP identity and access management
- Containerization of applications
- HSDP's Cloud Foundry application hosting/build environment: A commercial Cloud Foundry environment for cloud-native development that meets regulatory requirements to support you in rapidly developing and testing applications
- Self-service model

APIs that enable developers to consume underlying orchestrated services.

- Abstraction layer on the cloud infrastructure and foundation cloud services that enables developers to consume the underlying services
- HSDP uses APIs, industry standards, such as OAUTH2, and healthcare standards, such as HL7 and FHIR, to reduce your development effort.

Full Operations support from HSDP: 24/7, 365 days a year support to configure, maintain, monitor and ensure operational availability of HSDP and the solution you are hosting on HSDP.

- Vendor management
- Configuration and maintenance of orchestrated, containerized, healthcare-compliant infrastructure
- 24/7 support to enable operational availability of orchestrated, containerized, healthcare compliant infrastructure
- Incident Management that complies with ITIL standards
- Continuous monitoring of the performance and availability of the platform, including cloud infrastructure, custom services, and applications
- Maintenance of HSDP infrastructure and software within expected service level commitments

HSDP cloud expertise: Expert support for your cloud development.

- Technical and business documentation and code samples on the Client Experience Portal
- Cloud development expertise to support developers in designing interoperable, secure, cloud-based microservice architectures
- Curated and moderated Slack channels for topical questions and knowledge sharing by the HSDP ecosystem community

Key components of HealthSuite digital platform

Consumer and healthcare solutions

Information security management system

Privacy, security and regulatory controls and operational support.

24 x 7 operations support

APIs

Enable you to consume services

Cloud expertise

Orchestrated cloud infrastructure

Choose what you need, pay only for what you use

Share **Analyze** **Store** **Authorize** **Host** **Connect**

Compelling benefits
of Philips HealthSuite digital platform

Competition in the consumer and health technology space is fierce and we have a lot to do, not only in the ways we bring innovation to our customers. We must also continue to innovate the way we operate by enabling fast, agile, quality-focused global teams.

Philips businesses and our partners recognize the need to operate in the cloud and its importance to future business strategy. Philips HealthSuite digital platform is your secure partner for fast, successful, expert entry to the cloud. It has been developed to offer 4 key benefits:

Security

HSDP reduces the significant risks of financial impact and loss of credibility due to privacy and security breaches.

You cannot afford a data breach. Any loss of your customers' sensitive data will result in significant financial impact and loss of credibility for your business. Unfortunately, cloud infrastructure vendors only provide compliance for the core infrastructure, leaving you to take responsibility for the compliance and operations of the platform and application layers.

HSDP safeguards health and other sensitive data in the cloud through a certified Information Security Management System; specific security services within HSDP; external audits and penetration testing; privacy, security and regulatory controls; and operational security. HSDP also maintains an extensive set of external compliance certifications and attestations to provide objective evidence of compliance to security and privacy regulations such as ISO 27001/18, SOC2, and HITRUST.

Speed

HSDP decreases your time to market. It offers ready-to-use cloud services, tools and resources to accelerate your development of connected consumer and healthcare solutions.

HSDP speeds your development time and your transition to the cloud, whether you have existing legacy products that you want to move to the cloud or want to develop cloud-native applications, or both.

HSDP gives you services, technical tools and resources optimized for the co-creation and rapid development and deployment of connected consumer and healthcare applications. HSDP provides a curated marketplace of foundation cloud services, such as databases and queues. In addition, it offers specialized services to support the breadth of solutions that Philips and our partners are developing.

Simplicity

HSDP removes the complexity of building and managing your own healthcare compliant, orchestrated, secure, cloud infrastructure and platform.

We created HSDP to provide a shared expertise and full-managed cloud-based infrastructure and platform as a service to eliminate the burden of you having to develop and maintain it yourself.

HSDP solves the challenges stemming from the complexity of configuring, securing and managing a cloud infrastructure and the problems that can arise from errors in doing so. Moving to the cloud is our shared goal at Philips. The configuration and maintenance of an orchestrated, containerized, healthcare compliant cloud infrastructure is a complex and massive undertaking.

Savings

HSDP reduces your expenses. It saves you the cost of hardware and software, compliance, and staff by providing a shared, fully-managed cloud infrastructure and platform.

Building, maintaining and monitoring a regulatory compliant cloud platform is expensive – there are time commitments and costs associated with the hardware and software infrastructure and staff with relevant expertise. Using HSDP reduces those costs. HSDP is designed so that you have the flexibility to use only the services you require and pay for only what you absolutely need.

In addition, having Philips business and partners use a shared resource is cheaper than the combined cost of each business incurring the cost of developing, configuring, maintaining and monitoring a secure, regulatory compliant cloud platform.

HealthSuite digital platform in numbers

Billions of images archived

Petabytes of imaging studies archived for healthcare providers

Millions of sleep therapy patients supported

Millions of IoT devices connected to the internet via the HSDP Connect IoT Services

Dozens of Philips and third-party products in production globally

Millions of seniors supported with our wearable Lifeline service

Hundreds of features on the platform

“We have to be in the cloud in order to execute on our strategy and transcend traditional information silos. While other industries have been fundamentally disrupted, the real impact of information technology is only now being felt in healthcare with our ability to glean and differentiate data in all settings to provide seamless care.”

Jeroen Tas Chief Innovation and Strategy Officer

Host

Our core services for cloud-native development and managed infrastructure in order to deploy and continuously monitor applications performance and the health status of systems.

Host services provide managed infrastructure for hosting and the essential and basic managed services for hosted applications supported by SLAs and performance metrics.

Value

- **Marketplace of building blocks**: Commonly used services, including databases and queues, in an environment that meets regulatory requirements
- **Auditing and logging**: Enhanced debugging efficiency, traceability, and compliance with privacy, security, regulatory standards for all applications being developed
- **Specialized services**: Services to increase developers' visibility into application activity
- **Notifications and configuration**: Facilitations and loosely coupled integrations with other services
- **Environment for cloud-native development**: Environment that meets regulatory requirements to support you in rapidly developing and testing cloud-native applications

Specialized Services Features

Host service provides specialized services to facilitate the development of cloud-based applications.

- **Auditing** service offers a centralized management service for collecting, and querying audit messages that record data access and usage across applications built using HSDP in a secure manner. Use it to create and retain audit events across your proposition to help you meet regulatory requirements
- **Logging** service provides a centralized log management service for collecting, analyzing, and displaying logs for the cloud-native applications that you can use to analyze performance or bugs
- **Configuration** service offers a central building block for managing product and system configuration securely with tenant-based approach. This allows application changes to take effect with limited or no service interruptions
- **Discovery** service allows customers to dynamically discover and retrieve service endpoints (URLs) for their applications. Users, devices, or services can retrieve the (set of) services and corresponding URLs that have been configured for their applications. Currently available only for HSDP services
- **Notification** service provides an event notification mechanism for HSDP-based applications in a service-to-service deployment model where producers or subscribers could be HSDP internal components, HSDP based applications, or HSDP interacting with third-party applications
- **User Preferences** service provides a managed key-value storage mechanism, allowing application developers to extend user profiles with individual user preferences and default application preferences

Infrastructure Services Features

HSDP provides a variety of managed HSDP and 3rd party databases and queues in a regulatory compliant environment.

Managed infrastructure services

- **Orchestration capabilities** enable dependent services to work together seamlessly with HSDP's IAM
- **Abstraction layer** Allows developers to consume the underlying services enables HSDP to add services from different vendors
- **APIs** may have operations restricted to meet security, privacy and regulatory requirements
- **Services are updated** to reflect changes in the infrastructure
- Note: HSDP also offers raw brokered storage services for client needs outside of these platform offerings

Examples of managed infrastructure services

- **Databases**: RabbitMQ, RiakKV
- **Service Brokers**: Dynamo DB, RDS Service Broker, Redis Sentinel Service Broker, Vault, Autoscaler
- **Storage**: Archive Storage

Cloud Foundry Features

HSDP offers the Cloud Foundry environment to support your development and testing of cloud-native solutions.

Environment for cloud-native development

- Environment for cloud-native development
- The preferred way to develop cloud-native applications on HSDP
- Meets privacy, security, and regulatory requirements
- Makes it faster and easier to build, test, deploy and scale applications
- Makes it easy to deploy persistent services like databases with service brokers
- Focus on your application. Cloud Foundry provides the framework, language, and operating system

Capabilities for Developers

- **Role based developer management** capabilities grant developers, auditors, and operators the roles they need
- **Application health monitoring** so that if your application fails, Cloud Foundry will automatically restart it
- **Rapid horizontal scaling** enables you to use HSDP autoscaler to automatically scale your application, or control scale manually
- **Deploy** your Docker image to Cloud Foundry
- **Monitoring and alerting** enables you to receive email or SMS if your application is having trouble
- **Application performance metrics, centralized logging** and **automatic load balancing**

Consult hsdp.io for details

Authorize

Our secure identity and access management with a unified view into security policy, authorization, consent and data privacy.

Authorize services provide Identity and Access Management (IAM), the secure, centralized mechanisms to manage identities, authentication and authorization of users, services and devices and enable access control. It also includes Terms and Conditions Management to manage consent and ensure data security and privacy.

Value

- **Enterprise-identity approach**: IAM provides capabilities for harmonizing multiple applications built on HSDP, enabling clients to use a single identity across multiple applications
- **Standard identity management workflows**: standards-based identity, authentication and authorization capabilities to eliminate redundant, error-prone, and often incomplete (re)-implementation of standard workflows
- **Cross-platform integration**: Centralized set of enterprise identity and access management mechanisms that enable identity integration across consumer or healthcare applications built on HSDP
- **Cross-infrastructure integration**: access across the HSDP cloud infrastructure with a single credential
- **Collaboration with third parties**: Support integration and collaboration with third-party applications and services through federation and single sign-on capabilities

Features

- **Identity Management** services enable the management and verification of identities across multiple applications built on the HSDP
  - Creation and management of identities for users, devices, applications, and services
  - Creation and management of groups, roles, permissions, and organizations to model the desired organizational structure and role-based access patterns
- **Authentication services** provide mechanisms for verifying identities and managing passwords and policies,
  - Verification of identities based on OAuth2 authorization grant types (code grants, authentication code grants, and client credentials), JSON Web Token (JWT) grant type, and client credentials
  - Two-factor authentication based on one-time password (OTP)
  - Identity federation with third-party identity systems through OpenID Connect and SAML2
  - Social sign-on support with Facebook and Google
- **Authorization** services enable flexible role-based authorization and access control
  - Authorization of identities based on group membership to ensure controlled access to data by identities with specific roles
  - Token management and policy management
  - Consumer self-registration with account management and password management, including standardized policies for expiration, history, and complexity
- **Terms and Conditions Management** service provides a mechanism to control and track user acceptance of terms and conditions documents. This service stores and manages URLs of application terms and conditions and enables a workflow to enforce acceptance of the latest versions

Consult hsdp.io for details

Connect

Our secure and scalable IoT services to manage, update, monitor and collect data from smart devices.

Connect services manage, update, remotely monitor, and collect & store data from smart devices; ranging from consumer wearables to large medical-grade systems, both Philips and 3rd party.

Value

- **Device management**: Highly scalable and secure services to manage connected devices for remote service, diagnostics, software updates, messaging, and device control
- **Collect health and wellness data**: Collect, store, validate, correlate and broker both personal (health) measurements and observations as well as device information and data
- **Third-party data integrations**: Access a wealth of data from third-party services and devices through Philips' partnerships with other industry-standard platforms

Features

Device Management

- **Master Data Management** service administers the configuration of master data for devices including device hierarchy and grouping, authorization master data, and firmware update master data. Clients who use Connect services can use the API's to create, read, or update the master data configurations of their devices
- **Provisioning** service allows devices and mobile apps to obtain their unique identity and key dynamically 'over-the-air', eliminating the need for devices to be provisioned upfront in the factory with a unique identity. All consuming entities – users, services, or devices – require this unique identity and key to use HSDP services
- **Authentication and Authorization** service enables device authentication and authorization using the following steps. A device uses the identity and key provided during provisioning to obtain an access token from HealthSuite Authorize – Identity and Access Management using the standard OAuth2 protocol. With this token, the caller can authenticate itself at any other HealthSuite service and get authorized based on permissions configured in Master Data Management
- **Discovery** service allows clients to dynamically discover and retrieve service endpoints (URLs) for their application, based on the configuration in Master Data Management. This provides flexibility for developers to dynamically configure and change services based on application-specific business rules
- **Firmware** service enables clients to update the firmware or software of their devices or mobile applications in the field. This allows them to update their installed base 'over-the-air' with new features, updates, or fixes. Customers can configure a firmware update request in Master Data Management
- **Control** service is a highly scalable messaging service that allows devices and applications to exchange events or messages and to control devices remotely in an easy and secure way using the MQTT protocol to send and receive messages. Applications or devices publish events to 'topics' and the messages are distributed to devices or apps that subscribe to a topic. Control service also supports sending mobile push notifications to mobile platforms
- **Data Broker** service is a highly scalable and secure message broker that allows devices and applications to send data and have it distributed (brokered) to subscribed receivers. Devices or apps can publish the data over the MQTT protocol or use the APIs to send the data over HTTPS. Based on configuration in Master Data Management, the Data Broker service distributes the data to one or more destinations. This can include customer endpoints, as well as endpoints that are part of HSDP-Store services

Device Data Integration

- **Data Integration** services support cloud-to-cloud integrations with third party clouds that are not connected natively to the Connect services. These device data integrations for importing, validating, and ingesting observations and measurements from Philips and 3rd party devices and services into HSDP. Includes Validic, Qualcomm 2Net and Samsung ARTIK

Consult hsdp.io for details

Share

Our standards-based interoperability between enabled apps and devices with third party systems via FHIR and HL7.

Share services enable you to build standardized interfaces between external systems and enabled applications and devices to facilitate cross-enterprise integration.

Value

- **Rapid and scalable integration**: Provides a high performing integration engine with many built in capabilities to provide semantic interoperability, connecting On-premise with the cloud API based systems
- **API based flexible framework**: Out-of- the-box support for REST based APIs, with support for a variety of message mapping and routing capabilities and custom integration to standard and application-specific workflows
- **Flexible messaging format support**: Supports variety of messaging formats, such as HL7 (version2 and 3) to HL7 FHIR, and enables integration with systems based on well-defined XML, JSON and any other proprietary formats

Features

- **Share – IO Bridge** services provides secure, extensible enterprise integration frameworks for users to exchange information with hospital enterprise systems. It simplifies implementation of communications, message mapping, message delivery, data transformation, and routing of data across different systems and normalizes data to the platform; supports standard based messaging protocols like HL7.
- **Integration framework** offers an integration framework that enables standard methods for integrating clinical and non-clinical data from hospitals systems and EHRs with cloud-based consumer applications. This integration framework is extensible and supports client-specific customizations and extensions
- **HL7 based standard support** enables standards-based interoperability using HL7 based profiles and workflows such as:
  - ADT: Admit Discharge Transfer Message
  - ORU: Observation Result Message
  - ORM: Order message
  - RDE: Pharmacy/Treatment Encoded Order Message
  - VXU: Immunization Message
  - MFN: Master File Notification Message
  - PPR: Patient Problem Message
  - REF: Patient Referral Message
- **Integration support** provides support for integration using web services, REST, JSON, and XML
- **Multi-tenant deployment support** enables users to configure a service in a multi-tenant setup environment, allowing a client application to have data segmentation per end point within the same service
- **Security and encryption** encrypts data at rest and in transit. It enables HTTP(S)-based multi-way SSL handshake and token-based authentication for data exchange

Consult hsdp.io for details

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 opti-mized 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 API's** 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
- **API's for Administrators** to manage access control allow Administrators to define policies for users and groups, allowing access to S3 buckets and folders
- **API's 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

Analyze

Our framework to ingest and manage data, execute ETLs and analytics applications, and visualize data.

Analyze services provides a framework for ingesting and managing data, executing ETL's and analytics applications and quickly visualizing retrospective, prospective, predictive, and prescriptive data.

Value

- **More data, more insights**: Enables the development big data analytics solutions to derive predictions and meaningful insights
- **Simplification**: Reduces the complexities of building and maintaining distributed big data computing environments by providing a common set of tools to ingest, transform, and extract data for advanced data visualization

Analyze Features

The Analyze platform service has four types of services.

- **Data Ingestion Framework** is a set of micro-services that deliver reliable and high performance ingestion of data sets to the Big Data Platform service in a highly scalable way. The ingestion framework can receive data through a variety of protocols, classify the data received (including validate that it conforms the canonical type definitions and quarantine invalid data) and extract business metadata, aggregate and package sets of data for efficient downstream batch processing and copy data from one storage system to another
- **Data Storage** of data for analysis is provided in S3 with support for multi-tenancy. In addition, it offers provenance to support detailed data processing traceability
- **Data Processing Frameworks** enable the creation, deployment and execution of data processing pipelines through a set of primitives/SDK to integrate newly ingested data with existing data and apply transformations as determined by data processing pipelines (extract, transform, and load)

Data Processing Frameworks Features

The Analyze - Data Processing framework, introduced above, is available in different formats, with similar capabilities, to suit your data processing needs.

- **Big Data Platform** (BDP) is a version of the data processing framework that is a Hadoop-based compute environment for processing large volumes of unstructured data
- **Data Warehouse and OLTP** is a version of the data processing framework that is optimized for processing large volumes of structured data via a data warehouse, or small volumes of structured data via an OLTP system
- **Data Ingestion Integration** this service connects to the Analyze – Data Ingestion service to allow integration of newly ingested data with existing data and apply transformations
- **Data access** is via a set of capabilities to retrieve processed data securely to enable end-user applications
- **Access control** supports the creation of new users, updating of profiles, granting or revoking access, deactivation of accounts, the import of new user identities, and synchronization for federated access through the integration of Authorize - IAM
- **Logging and error handling** supports logging of data processing events with error handling capabilities through the integration of Host - Logging

Consult hsdp.io for details

By integrating and combining consumer and clinical data we're able to create smarter and more meaningful connected consumer and health solutions.

Powering innovations
with HealthSuite digital platform

Philips HSDP gives you and your developers the technical tools and services to **create innovative consumer and healthcare applications** that can deliver a more personalized care experience for individuals and health and wellness professionals. It represents a new era in connected health and care, as healthcare continues to move outside the hospital walls, and into our homes and everyday lives.

HSDP clients have used HSDP's regulatory compliant cloud infrastructure and platform as a service to achieve their vision for connected solutions for consumers and healthcare. The following case studies demonstrate the versatility of HSDP and the myriad of ways in which you can use the HSDP's cloud services you select for your cloud-based solution.

Get Started
with HealthSuite digital platform

Leverage platform services depending on your businesses' cloud development stage
Your specific needs and how you leverage the capabilities of HSDP will vary depending on where you are in cloud development, from proof of concept to production ready.
Choose what you need. Pay for what you use.

Legacy solutions
If you have a legacy application or solution that you want to move to the cloud, you can host your application on our compliant cloud infrastructure and receive 24/7 operational support.

New Cloud-Native Development
If you are ready to begin creating a new solution from scratch, you can leverage HSDP's managed, compliant cloud platform as a service to build and deploy your new solution using our Cloud Foundry environment and HSDP platform services.

Combination of Cloud-Native development and legacy applications
If you have a mix of legacy and cloud-native development, you can use our services in flexible ways to address your varying needs. Take advantage of containerization, for example, that allows you to use your legacy components in combination with cloud-native services.

Ready to learn more or to start using HSDP services?

Step 0: Want to understand HSDP?

The HSDP team is available to give you an introduction to HSDP.
You can contact us at **HSDP-gettingstarted@philips.com**

Step 1: Discuss your business and technical needs with HSDP

The HSDP team is here to provide guidance and answer your questions about HSDP. They will walk you through HSDP services and understand your vision for your solution, your development needs, and your timelines. Based on this needs assessment, they will partner with you throughout the process, to identify appropriate HSDP platform services. Whether you are at proof of concept stage or have a production-ready solution, we will work with you to find the services that meet your development stage and budget.

Step 2: Get an Account for the HSDP Client Experience Portal

We invite you to use the HSDP Client Experience Portal at **https://www.hsdp.io/**
First you will need an account.

- **Philips**: Use the 'Create an Account' page on the HSDP Client Experience Portal at **https://www.hsdp.io/user/registerto** register for an account using your Philips email address
- **Philips partner**: HSDP will enroll you for an account for the HSDP Client Experience Portal at **https://www.hsdp.io/ and send you your credentials.**

Step 3: View HSDP documentation

Once you are registered for the Client Experience Portal at HSDP.io, you will be able to review HSDP service descriptions, release notes, API documents and other technical documentation available on the portal. This information will be useful as you decide which HSDP platform services interest you the most.

Step 4: Onboard to select HSDP services

You are ready to onboard. Contrary to popular belief, you are not onboarded to all existing HSDP services at once – that is the value of the pay-per-use model in which you choose which services you need and pay for only what you use. You will select specific services, which are relevant for your development needs, and be onboarded onto those services.

Step 5: Access HSDP services

During onboarding, HSDP will give you access to an instance with the HSDP platform services requested. You will be able to use the APIs and the technical resources on the Client Experience Portal to learn about the services hands-on, with HSDP Support available to assist you. HSDP will work with you through on all onboarding documents and activities.

www.philips.com
October 2018