The HealthSuite Platform

Helicon Health offers the The Philips HealthSuite Platform (HSP) under GCloud13. HSP provides the secure cloud infrastructure hosting and Platform-as-a-service solution for Philips businesses and partners. The platform is deployed globally in multiple AWS data centers to enable approximately 100 business customers around the world.

We developed HSP to address the industry challenge of personal health and wellness data scattered over many applications, devices and systems in multiple places and formats. The platform unleashes the value of the data by allowing access to data and data integration on a patient across different episodes of care and health systems. By integrating and combining consumer and clinical data our customers are able to create smarter and more meaningful connected health solutions; solutions where consumers and care providers are able to look at the full clinical context of the individual that includes a wide range of data such as monitoring data, self-management data, health records and genome data.

HSP is designed to help you overcome the challenges associated with moving consumer and personal health applications to the Cloud, so that you can turn your efforts to harnessing its power and focus on delivering innovative, value-adding products, services and solutions. Leveraging our Philips expertise and experience in both the clinical space and consumer technologies, we are helping consumers, healthcare providers, payers, and companies address the challenges and opportunities they face and applying our unique ability to develop and deliver solutions that span the health continuum.

The HSP Platform Services are a tailored set of tools and resources optimized for the co-creation and rapid development of consumer and healthcare applications. The six types of platform services, each of which encompasses multiple services, provides capabilities for developing consumer and healthcare solutions for a large number of stakeholders with varying data-related needs. This enables you to connect people, devices, technologies and data across the health continuum from consumers to clinicians, administrators, and researchers and facilitate collaboration on health and wellness. Within a single platform, HSP gives you capabilities to address your customer's needs:

- Consumers, patients, and informal caregivers need capabilities to enable them to access to and control of personal data sharing
- Health and wellness providers need capabilities that will support having actionable clinical data where, how and when relevant
- Administrators need analytics capabilities to help manage patient populations and reduce financial risks
- IT professionals need capabilities to address interoperability, privacy and security to ensure secure data exchange
- Developers need open APIs, leverage industry standards, and a compliant cloud infrastructure
- Researchers and data scientists need capabilities to support analytics, machine learning, artificial intelligence

The services within HSP fall into three categories (see figure 1):

- **The Cloud Infrastructure**. This consists of the managed Cloud infrastructure and the Cloud Foundry environment that HSP provides for Cloud native development. HSP uses AWS for its underlying cloud infrastructure and builds on AWS' six key benefits of easy-to-use, cost effective, secure, reliable, scalable and flexible cloud infrastructure.
    - 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 HSP identity and access management
    - Containerization of applications

- HSP's Cloud foundry application hosting/build environment: A well-supported, Cloud Foundry environment for Cloud native development that meets regulatory requirements to support you in rapidly developing and testing applications
- Self-service model
- Traditional managed and unmanaged windows hosting

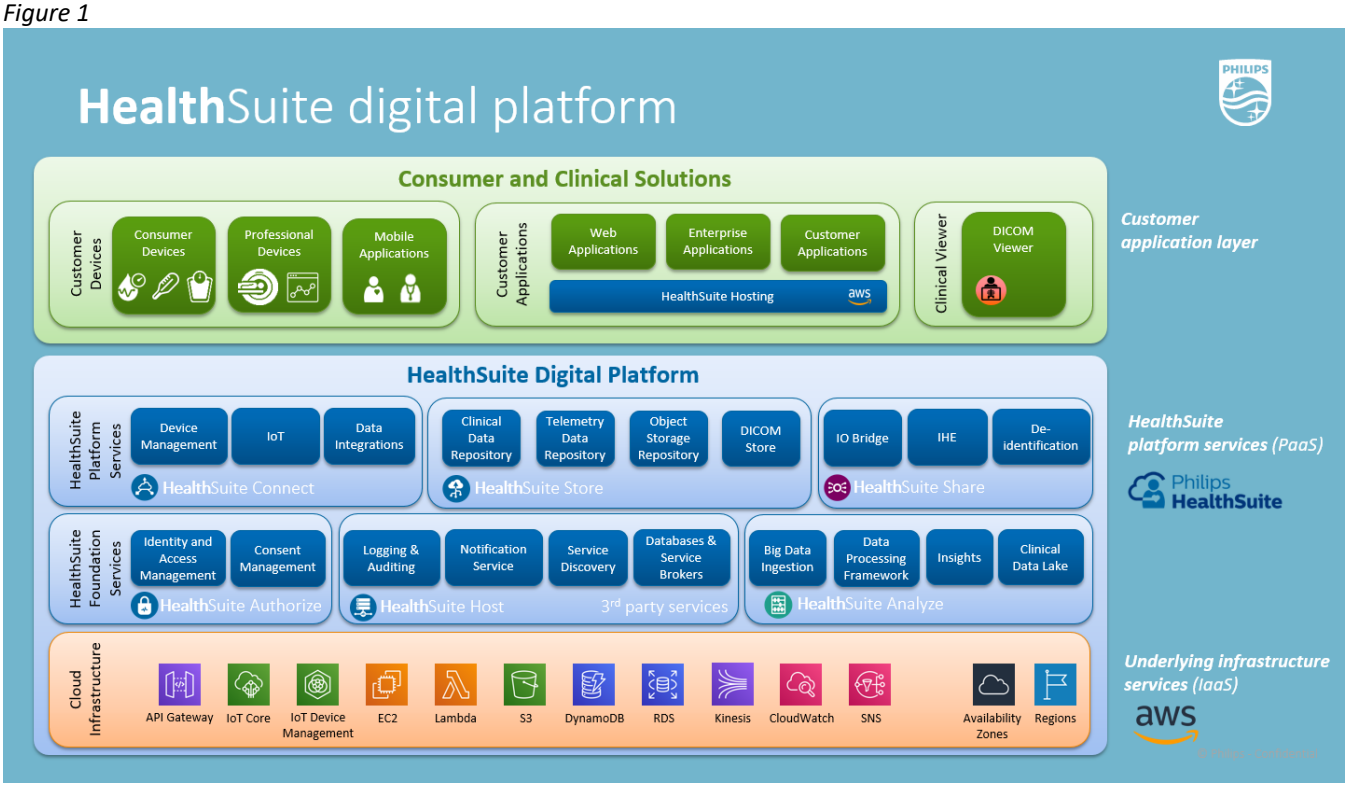
- **Foundation Services**: Specialized services and managed Philips and 3rd party Cloud databases and queues for development and debugging; Authorize services for identity and access management; Analyze services for data science, data ingestion, storing and processing of big data.
  - Host services provide managed infrastructure for hosting and the essential and basic managed services for hosted applications supported by SLAs and performance metrics:
    - RabbitMQ, Dynamo DB, Amazon RDS Service Broker, Redis Sentinel Service Broker, RiakKV, Amazon Redshift Service Broker, Elasticsearch, Vault, Autoscaler, Archive Storage based on Amazon Glacier.
  - Host Foundation –
    - Authorize services: Identity and Access Management (IAM) secure, centralized mechanisms to manage identities, authentication and authorization of users, services and devices, federation and enable access control
    - Audit, logging, discovery and notification services

- **Application platform services** that are designed for developing consumer and healthcare solutions.
  - "Connect" for Device Management/IoT
    - Developed in collaboration with AWS with a foundation built on AWS' broad and deep Internet of Things (IoT) and serverless services the Connect IoT suite of services provides Internet of Things device management and connectivity capabilities for devices and applications in health and non-health propositions, ranging from consumer-grade wearable devices and sensors to large, professional systems and equipment. The Connect IoT suite provides a range of highly scalable and secure services to manage, update, and monitor smart devices, sensors, and applications.
    - Integrated edge compute capabilities based on AWS' Snow Family of devices providing IoT capabilities as well as secure ingestion of data to the cloud.
  - "Store" our different managed data repositories
    - Clinical Data Repository (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
    - Telemetry Data Repository (TDR) a service for storing user data and observations, as well as device data. Optimized for speed, throughput, reliability and scalability
    - S3 Credentials Service provides the ability to integrate the IAM service directly to Amazon S3 storage for uploading and downloading data.
    - DICOM - Full support of DICOM standard QIDO, WADO and STOW services
  - "Share" our IO Bridge services for interoperability

    Secure, extensible enterprise integration frameworks 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. HL7 and FHIR based standard support enables standards-based interoperability using HL7 and FHIR based profiles and workflows

- ”Analyze”
  - 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.
  - HealthSuite Insights platform – a set of tools and technologies to address the advancing adoption of analytics and artificial intelligence in healthcare. The platform addresses the complete ‘end to end’ process of analytics and AI asset creation, deployment, and support.
  - Clinical Data Lake - for storage of management of research data, including services for de-identification of data
  - Upcoming support for Amazon SageMaker, which provides the ability to build, train, and deploy machine learning models quickly in applications, on-premises or in the cloud.

Figure 1



Integrated security, monitoring and operations

HSP has implemented its Information Security Management System and the privacy and security controls, audits and operational security to ensure that the Cloud infrastructure and platform as a service offering are fully compliant with healthcare regulations. In addition, HSP has a quality management system to ensure that it meets GxP requirements.

Our customized, orchestrated platform services with APIs to address the needs of healthcare and consumer solution development. Our orchestration capabilities ensure that dependent services work together seamlessly within our robust HSP identity and access management.

Applications can be developed natively on HSP through our Cloud foundry application hosting/build environment: A well-supported, Cloud Foundry environment for Cloud native development that meets regulatory requirements to support you in rapidly developing and testing applications. Alternatively, we provide mechanisms to deploy applications in secure containers and via traditional managed or unmanaged hosting. Some of the features of our application development environment includes:

- Self-Service – Ability for customer self-deploys
- Automatic integration
- Integral Fault Recovery
- Strong per Customer isolation – process, security, operational
- Curated Buildpacks and 'Roll your own' Options
- Abstraction compute layer 'true serverless'
- Dynamic Scaling
- Automatic SSL, DNS, IP Routing, Security Group Mapping & Management, and more
- **Monitoring offering:**
    - Instrumentation and dashboards for your application and operating environment
    - Capability for Application level monitoring
    - Infrastructure level monitoring
    - Capability for End-user experience performance monitoring

The Cloud infrastructure is always changing due to failures, changes and security patches, just like a traditional data center. Consequently, full Operations support from HSP entails 24 x 7 support to configure, maintain, monitor and ensure operational availability of HSP and the solution you are hosting on HSP. Our operations support includes:

- Configuration and maintenance of orchestrated, containerized, compliant infrastructure
- 24x7 support to enable operational availability of orchestrated, containerized, compliant infrastructure
- Incident Management that complies with Philips standards
- Continuous monitoring of the performance and availability of the platform, including Cloud infrastructure, custom services, application
- Maintenance of HSP infrastructure and software within expected service level commitments (SLAs)
- Platform Operations
    - Call Center / Support Operations
    - Platform Health
    - Monitoring
    - Updating
    - Capacity Management
    - Reactive Services
    - Custom Support Services
    - Vendor Management
    - Security Surveillance/Testing
    - Image Curation
    - Broker Lifecycles
    - Integrated Tooling
    - Incident Management
    - Spend Optimization for both Platform and Non-Platform Services

The Cloud expertise of HSP includes technical and business documentation on the Client Experience Portal and consultation on designing interoperable, secure, Cloud-based microservice architectures. Curated and moderated Slack channels for topical questions and knowledge sharing by the HSP ecosystem community.

Infrastructure multi tenancy

HSP is built on top of Open Source Cloud Foundry and is designed to operate as a multi-tenant environment. Cloud Foundry is used as the core application hosting platform that is used to deliver the applications and services that make up HSP. The environment itself provides several differences from traditional hosting solutions and managing risks by abstracting key elements out of the "application" stack and making them available as part of the underlying platform.

Cloud Foundry is divided into logical Organizations (orgs) and spaces using role-based access controls to grant users permissions within an org and space.

- **Orgs -** A Cloud Foundry **org** is a logical container for a development group that allows multiple users to collaborate on development projects. Each digital proposition or Platform service will have only one Cloud Foundry organization. Users in an org share resources within an environment, but the org manager is ultimately responsible for all resources within their org, including its space structure and users.
- **Spaces -** Cloud Foundry orgs are subdivided into **spaces**. Best practice dictates spaces map to development areas such as integration, testing, staging, and/or production. Each org starts with a dev space; it is the responsibility of the org manager to create additional spaces to meet the needs of their development team. Applications and services are scoped to a space. User permissions are individually granted for every space. To give a user the same permissions in multiple spaces, they must be assigned separately in each.
- **Roles -** Org managers control the user permissions within their org and spaces. HSP Operations sets up the initial org and grants permissions to the org's first manager. The rest of the user permissions are then managed independently by the org manager. The responsibilities of org managers are laid out more fully in the chapter on expectations for org managers.

Additionally, applications are deployed into containers that provide isolation from other applications running on the platform. These containers store application configuration, environment variables, and service credentials in an encrypted database table while also conforming to network traffic rules. HSP is deployed in manner that leverages multiple availability zones, this construct allows for full redundancy at all hosting layers and allowing for full recovery from a disaster.

Next level of detail for selected services

Next level detail on a few of the specific services: (full details and specifications are available upon request.

- **Auditing** service offers a centralized management service for collecting, and querying audit messages that record data access and usage across applications built using HSP 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
- **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 HSP services
- **Notification** service provides an event notification mechanism for HSP-based applications in a service-to-service deployment model where producers or subscribers could be HSP internal components, HSP based applications, or HSP interacting with third-party applications
- **Identity Management** services enable the management and verification of identities across multiple applications built on the HSP - 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
- **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 HSP 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 HSP-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 HSP. Examples includes Validic, Qualcomm 2Net and Samsung ARTIK

- **Clinical Data Repository Features (FHIR Server)** 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. Includes:
    - **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 HSP, 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

- **HSP Analyze details**
  - **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 by Amazon 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)
  - **HealthSuite De-Identification** removes personal and sensitive information from data in order to ensure the privacy of patients when data is made available for data science research. The service supports DICOM data de-identification, structured EMR data (Q1 2020) de-identification as well as free-text de-identification (Q2 2020). De-Identification service employs novel deep learning techniques to automatically detect personal and sensitive information. It is a highly configurable pipeline, allowing privacy officers to configure how to treat different types of personal information, to what extent de-identification should occur, when it should run and how often. The service also supports an optional re-identification sub-service, which would keep track of a mapping table in a secured environment and allows re-identification of the data at a later time, for example when medical regulations require certain scientific results to be communicated back to patients.
  - **Clinical Data Lake** is a micro-service for the management of research data. The Clinical Data Lake enables AI development in the medical field and provides the infrastructure that is needed to house very large datasets in a regulatory compliant manner. These data types require fine-grained access management to enable collaboration across the globe without compromising the safety of the data. For data to be useful for machine learning and data science, it needs to be well-curated. The Clinical Data Lake delivers on these needs by combining a number of HSP services. The clinical data lake supports ingestion of heterogenous data sources in a single environment using S3, pre-processing of the data to clean up, normalize and index it in FHIR. Research managers can organize the data into different clinical studies, create cohorts out of the data and share those cohorts with data science teams, which can use the data to develop and validate AI propositions with.
  - **HealthSuite Insights Workbench** a data science workbench for the development and deployment of AI models developed in Philips, packaging a variety of open-source tools such as Jupyter Notebook, R studio, TensorFlow and Sacred to provide an integrated environment for data analysis and AI model training and

validation. Just like the clinical data lake, this platform is built on HSP to benefit from the horizontal scalability from Amazon Web Services.

- **HealthSuite Insights Runtime** a machine learning runtime where machine learning models can be deployed using the “one-click deploy” feature that makes any Python or R model available as a web service through a managed REST-API. With this method even the toughest scalability demands can be met by leveraging HSP’s and Amazon’s infrastructure.

PHILIPS

HealthSuite

platform

Managed Device Connectivity

Philips HealthSuite Platform

January 2022 | version 1.6

Enabling remote connected care

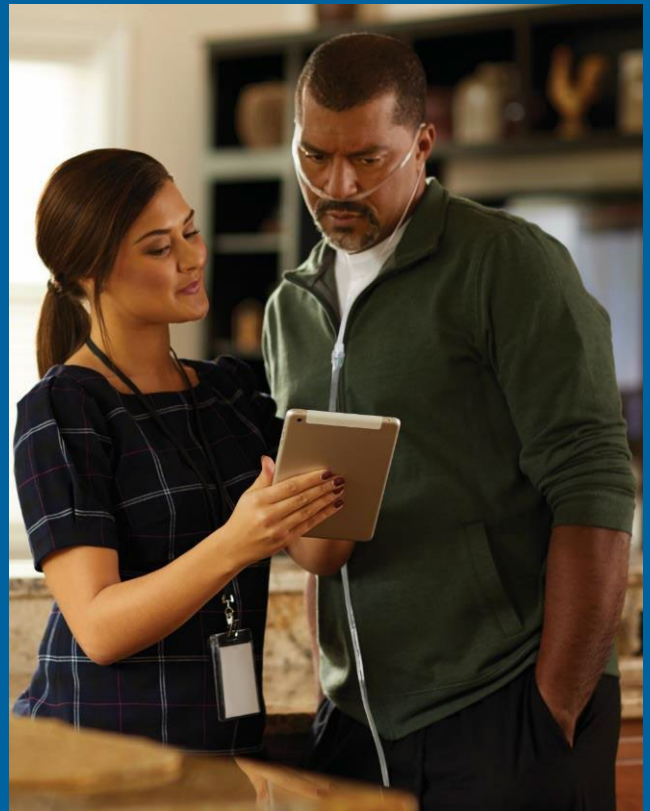
Smart connectivity and device management

Get patient and device data into the cloud in an easy-to-commission, scalable and secure way

HealthSuite
Managed Device Connectivity

Remote Patient Monitoring | Connected Health

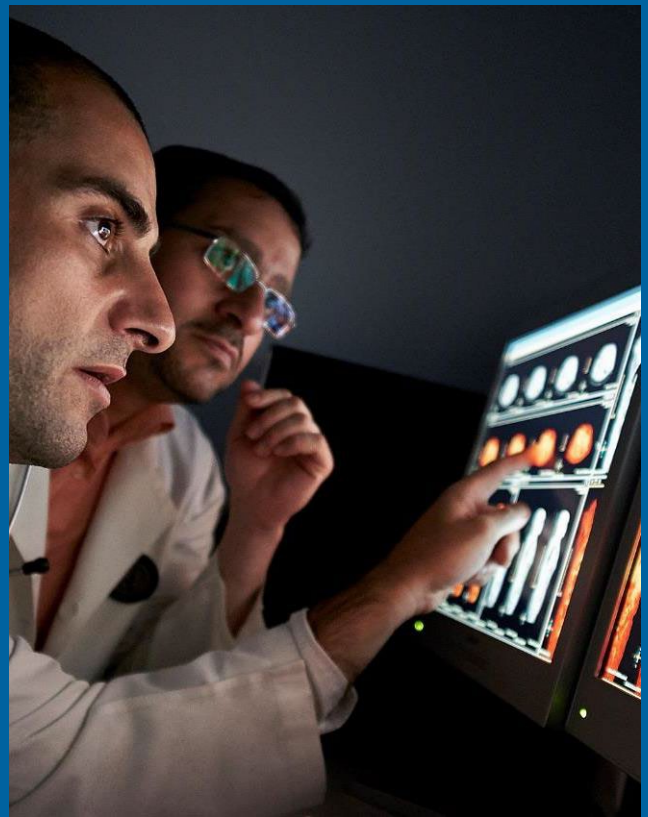
Enabling remote care



Remote patient monitoring programs can provide scalable, tailored pathways to:

- Help reduce cost and improve quality for ‘frequent fliers’
- Tailor personalized, longitudinal care plans to help improve self-care for patients with complex chronic conditions
- Help patients regain health stability via daily monitoring to reduce readmissions
- Increase access to care and help improve patient satisfaction

Clinical Trials | Contract Research
Remote data collection



Clinical trials increasingly use connected devices to ease the collection of data and improve the patient experience:

- Capture patient and device data more efficient and cost-effective
- Reduce the burden on patients through hassle free installation and daily use
- Direct feedback and insights for both research organizations (CRO) as well as patients

Medical Devices Manufacturers
Ecosystem building

People are looking for new ways to stay healthy, live well, and care for their loved ones at home:

- Integrate your devices to become part of a large ecosystem of consumers and patients, healthcare providers, and medical professionals
- Leverage Philips HealthSuite cloud infrastructure to reduce time-to-market for your devices and significantly reduce operational costs and burden

Managed Device Connectivity solution

Get (out-)patient data from wearable and peripheral devices into the cloud directly or through gateway devices

Solution provided as part of the HealthSuite platform that offers **smart connectivity and device management services** to create simple-to-commission and zero user action connected care solutions

We offer various ways to get device and patient data direct into the cloud with or without the use of managed gateways, mobile phones or tablet apps

Once inside the cloud, the HealthSuite platform services enable you to use the data in your innovative and secure connected health propositions

Why Managed Device Connectivity as a service?

Our customers in Primary care, Patient monitoring, Pharma, Clinical trials, are facing challenges in how to efficiently monitor vital signs of their patients at home and how to get this data securely available in the cloud for processing

Philips has recognized this and has expanded its offering with a **Managed Device Connectivity** solution

- Provides a managed, cost-effective and secure means of getting out-patient data available in the cloud
- From there, customers can pull the data from the APIs directly into their own applications and/or forward the data via HealthSuite to a hospital/clinical information system
- Customers need not worry about the cellular integration and management: it can be integrated into the service and provided by Philips and partners
- Device provisioning and logistics can be supported through partners
- Easy integration with other HealthSuite services: account management or federation of hospital identities for both patients and professionals, FHIR compliant clinical data repository, analytics platform, etc.
- Can also be delivered as SDK-only for integration in customer applications.

- Customers pay-per-use for the service, which includes maintenance & support for the entire chain from device to stored data
- The service is priced based on active gateways per month, based on a fair-use policy for data transfer and storage
- The standard service includes a wide range of natively supported, off-the-shelf Bluetooth sensor devices, and a number of gateway platforms. Support for additional, bespoke devices or gateways can be offered on a T&M basis

Service models

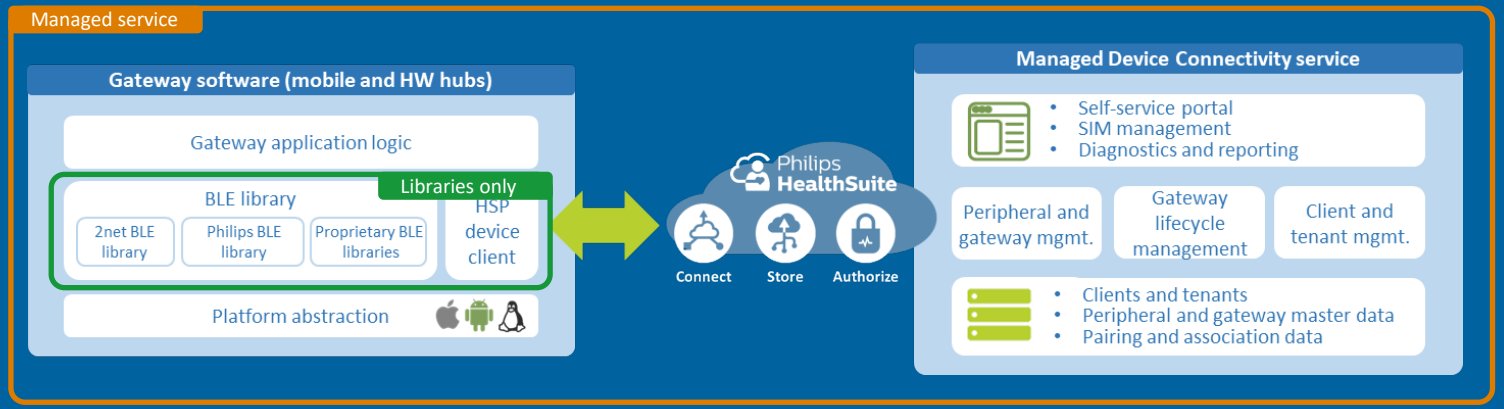
Based on customer need, the Managed Device Connectivity service can be consumed in two ways: as a fully managed, end-to-end service – or as software libraries only

Managed service

- Offered as a fully managed service
- Cloud-management of gateways and tenants, provisioning, (pre-)pairing, etc.
- Pricing based on # of active gateways per month
- Including use of HSP Connect IOT services
- Including technical support
- Option 1: including TDR storage
- Option 2: including cellular connectivity

SDK / Libraries only

- Provides libraries and documentation for integration with customer application; no cloud-management
- Pricing based on # of active gateways per month
- Including technical support
- Option 1: including TDR storage
- Option 2: including HSP Connect IOT services



Pricing models

The Managed Device Connectivity service is charged as a consumption-based service

- Customers pay-per-use for the service, which includes maintenance & support for the entire chain from device to stored data
- The service is priced based on active gateways per month, based on a fair-use policy for data transfer and storage
- The standard service includes a wide range of natively supported, off-the-shelf Bluetooth sensor devices, and a number of selected gateway platforms (mobile and fixed)

Service pricing

- Service pricing includes the license fee for the gateway software and usage of the underlying HSP services (IAM, IOT, TDR)
- Service pricing excludes the costs for the (HW) sensor devices, gateway devices, and mobile (cellular) connectivity costs
- Cellular connectivity is optional and can be offered by HSP direct or through partners
- Outside of the fair-use-policy, services are available against HSP prices

Sensor and Gateway devices

- The list of supported BLE sensor devices is continuously tested and maintained as part of the service
- Support for additional, bespoke sensor devices can be priced based on T&M
- Integration and maintenance of additional (bespoke) gateway devices can be offered on T&M basis

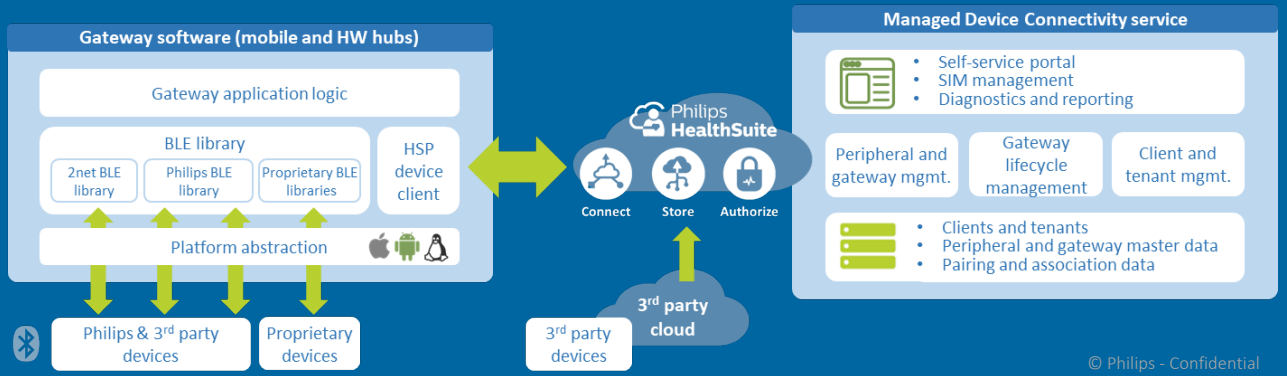
Feature overview

Gateways

- Can run on gateway / hub devices in different from factors
  - Stationary hub devices in patient homes or care facilities
  - Mobile devices that function as both gateway as well as patient-facing application
  - Medical devices with embedded connectivity
- Cloud connectivity based on Cellular, Wi-Fi, Ethernet or POTS [1)]
- Wide range of commercially available devices as well as proprietary devices
  - 16 categories: weight scale, thermometer, pulse ox, BPM, glucose, activity tracker, etc.
  - Supports standard Bluetooth GATT profiles; designed to easily support new devices
  - Integration of proprietary devices and protocols based on customer needs
  - Configuration of BLE devices: clock setting, credentials, data encryption keys [1)]
- Zero-touch / easy-to-use pairing with BLE devices
  - Support for devices using BLE 4.0 and upwards
  - Pairing and bonding mechanisms focused on ease-of-use (Just Works, Passkey, etc.)
- Flexible device-to-gateway and gateway-to-patient pairing methods
  - Association to patient/tenant organization
  - White- and blacklisting of peripheral devices
  - Ability to add custom attributes
- Remote configuration of gateway behavior (device pairing, data buffering) [1)]
- Secure data storage in HSP Store or push to customer endpoints
- Integration with HSP Connect IOT
  - Secure authentication, device management, firmware update, service discovery

Cloud

- Client and tenant management
  - Self-service onboarding of tenants, incl. user management [1)]
  - Gateway and peripheral device configurations per tenant
  - Reporting on client, tenant, gateway-, and peripheral devices
- Gateway and peripheral management
  - Onboarding and management of gateway types and peripheral types [1)]
  - Configuration of gateway- and peripheral instances: tenant association, pairing behavior, white- and blacklisting, data endpoints, custom attributes etc.
  - Lifecycle management of gateways: software updates, factory reset
- Cellular connectivity management
- Operation through HSP self-service portal, or integration with customer portal through APIs



[1)] roadmap capabilities

Compatibility approach

The Managed Device Connectivity service includes a wide range of commercial ‘off-the-shelf’ Bluetooth devices

- The service supports the major Bluetooth (GATT) profiles to cover most standard sensor devices on the market
- In addition, several non-standard / proprietary protocols have been implemented
- The list of natively supported devices is continuously tested and maintained as part of the service
- Support for additional, bespoke sensor devices can be added based on T&M

We distinguish between the following levels of device support

Open ecosystem	Verticals
Gold • Controlled set of most popular devices in different categories, different price-points, different markets • Provided by trusted brands with stable lifetime and availability • Extensively tested as part of the service, including automated regression testing at every release	**Proprietary** • Devices using non-standard communication profiles that have been integrated on specific customer requests • Only available for use by other customers on agreement with owning customer • Devices are tested at regular intervals, as agreed with the specific customer
Silver • Large set (100+) of peripheral devices in different categories • Typical long-tail of a wide variety of brands and device types • Tested as part of the service; periodic re-testing but at lower frequency or when relevant for a release • May move to Gold level based on sufficient demand or T&M	

Philips / 2net integration

2net Integration Overview

What

Philips acquired 2net assets and select personnel from Capsule

When

April 17, 2020

Where

2net is now part of HealthSuite Platform (HSP)

Why

Acquisition provides investment protection and expanded connectivity capabilities designed to optimize patient data in support of better health outcomes

Client Benefits

Opportunity to **build and expand capabilities** on a proven, trusted cloud platform

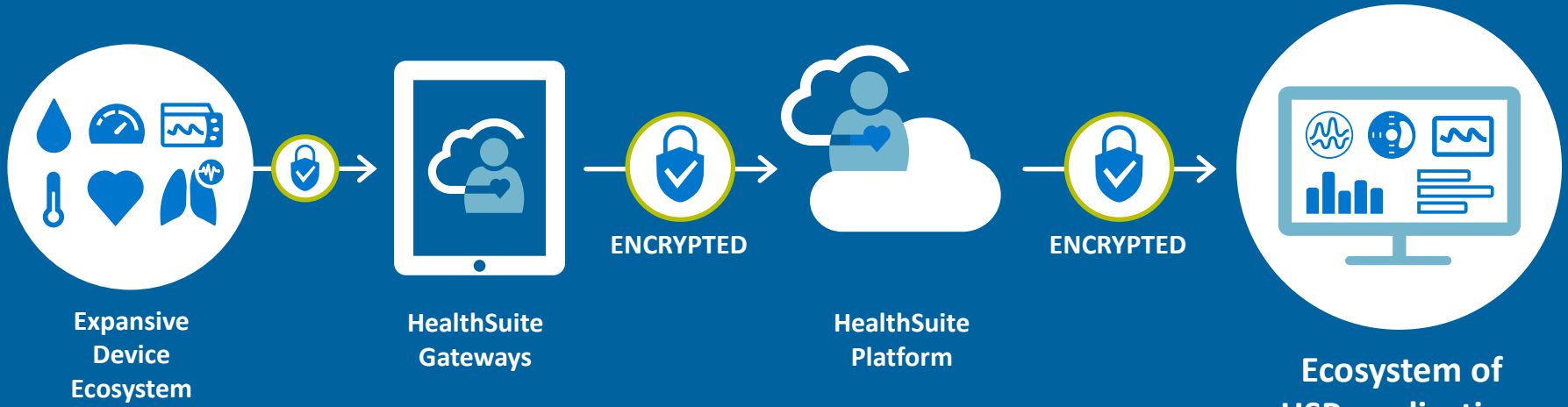
Confidently **invest in a scalable solution** focused on interoperability, security and compliance

Perfect match between 2net's device connectivity and Philips' strategy and position in medical device technology and cloud offerings

Leverage **Philips global network** of medical solutions and expertise that includes informatics, telehealth, diagnostic systems and healthcare consulting

Hubs and Gateways

Service Components



2net Hub Gen 2

Increased bandwidth and continuity with LTE Support

Secure M2M connectivity

Advanced Encryption Standard AES-256

Over-the-air upgrades
- *Application layer*
- *Security updates*
- *Patches*

Expanded memory
- *2GB for medical data*

Effortless user experience
- *Audible feedback*
- *Intuitive light sequence*

2net Mobile

Secure gateway

Designed to HIPAA privacy and security standards

Dynamic provisioning
Effortless multi-sensor setup

Embedded software module for OEM applications

Open architecture connecting to expansive ecosystem

Bring your own device (BYOD) flexibility

NEW 2net Hub Gen 3 (BioHub)

LTE Cat M1 / Cat-1 cellular connectivity

Bluetooth 4.2 and Wi-Fi 802.11a/c/n

Android OS

HealthSuite IOT connected
- *Secure connection*
- *Device management*
- *OTA updates*

USB ports for extensibility
- *Ethernet*
- *POTS*

Improved user experience
- *Touchscreen display*
- *Audible feedback*

Cassia Networks E1000/S2000

Enterprise Bluetooth Gateway

Long range, high-performance Bluetooth connectivity

Deployment and management through Cassia Access Controller

Allows integration of native app or server software

Several connectivity options

- *Ethernet*
- *Wi-Fi*
- *Cellular 3G/4G*

Devices Ecosystem

HSP Device Ecosystem

Device categories	16

Device types integrated	98

Including non-released integrations	199

Device Category	
Activity Monitor	2
Blood Glucose Meter	26
Blood Pressure Monitor	12
BPM Combo	3
Coagulation	1
Medication Adherence	3
Inhaler / Nebulizer	12

Device Category	
Insulin Pump	1
Pulse Oximeter	5
Spiro / Oximetry	9
Oxygen Concentrator	3
Thermometer	4
Weight Scale	16
Wheelchair	1

Gateway Category	
2net Hub Gen 2	65
2net Mobile Android	51
2net Mobile iOS	11
2net Hub Gen 1	79

- **Device and application agnostic, open design**
- **One of the largest connected health ecosystems**

Activity Monitors

Omron HJ-721IT + Docking station

Striiv Fusion/Lite

Xiaomi Amazfit Bip

Xiaomi MiBand 3

Blood Pressure Monitors

Continua CERTIFIED A&D UA-767PBT

A&D UA-651BLE

FORA P20b

Indie Health 51-1490

Medisana BU540

Omron BP792IT

Omron HEM-9200T
Omron HEM-9210T

Soehnle Connect 300
Soehnle Connect 400

Welch Allyn 1500 series
Welch Allyn 1700 series

Combo Blood Pressure / Blood Glucose Monitors

FORA D40b 2-in-1

TaiDoc TD-3223

Glucose Meters

[1] Through Polytel Wireless Glucose Meter Accessories

Abbott FreeStyle Freedom Lite [1]

Abbott FreeStyle Lite [1]

Nipro / Trividia Health TRUE METRIX AIR

Entra MyGlucoHealth SmartBLE

LifeScan OneTouch Ultra [1]
LifeScan OneTouch Ultra2 [1]

LifeScan OneTouch UltraMini [1]

FORA G31b

FORA Test N'GO

Bayer Contour [1]

Bayer Contour NextEZ [1]

Bayer Breeze 2 [1]

Pulse Oximeters

Beurer PO60

ChoiceMMed MD300C228

ChoiceMMed MD300C318T2

ChoiceMMed OX200

Contec DMS50D-BT

Nonin 3230

Nonin Onyx II 9560

Spirometers

MIR Spirotel

Vitalograph Spirometer 4000 asma-1

Vitalograph Spirometer 4000 copd-6

Vitalograph Spirometer 4000 lung monitor BT

Thermometers

A&D UT-201BLE

Beurer FT95

Motorola MBP69

FORA IR20b Ear

FORA IR21b Ear & Forehead

Weight Scales

Omron Body Composition
HBF-206IT

A&D UC-351PBT-Ci

Continua CERTIFIED

A&D UC-352BLE

A&D UC-352BLE-V
A&D UC-352-BLE-CE

Continua CERTIFIED

A&D UC-355PBT-Ci

Continua CERTIFIED

Fitbit Aria

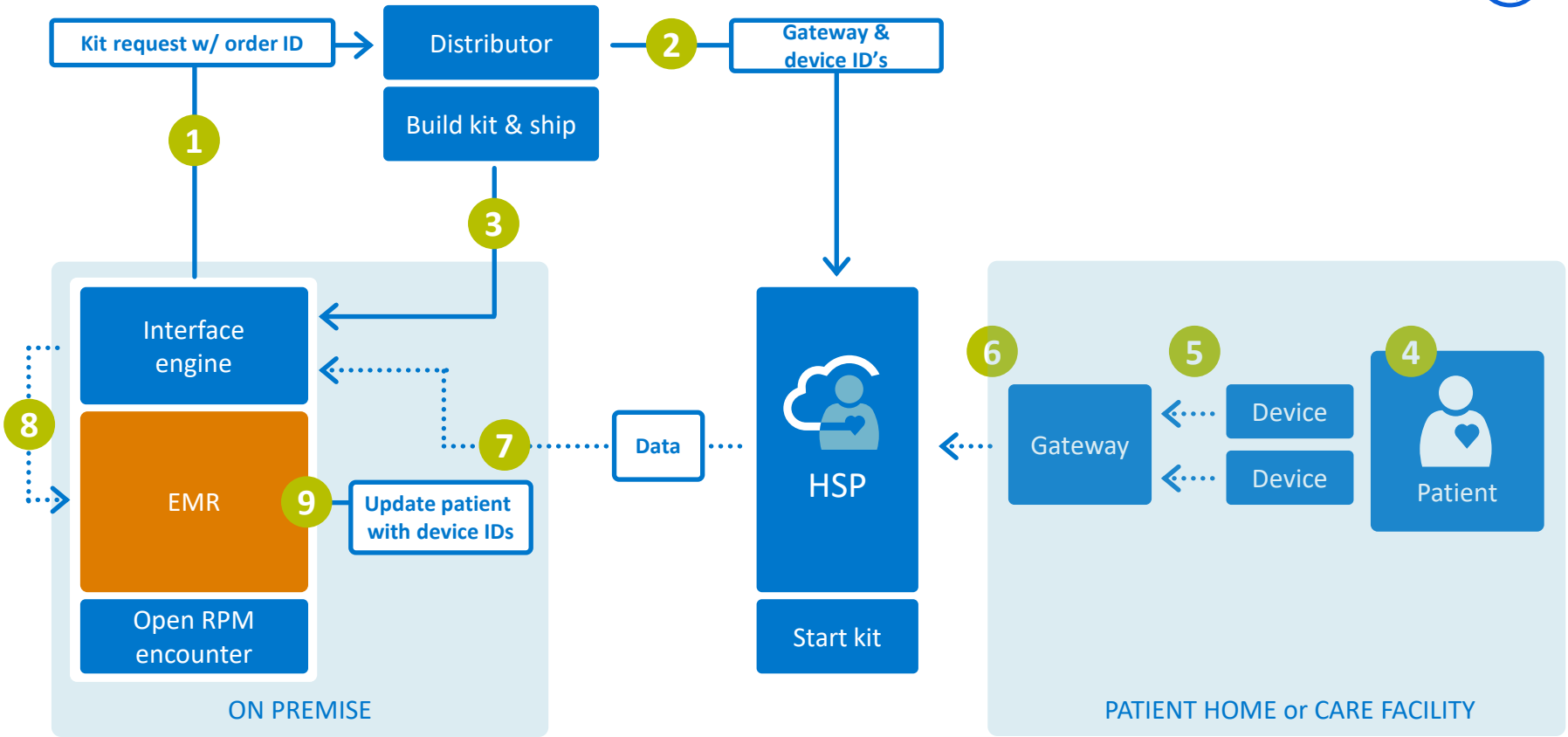
FORA W310b

Indie Health 51-102

MyFitnessPal

Workflow Options

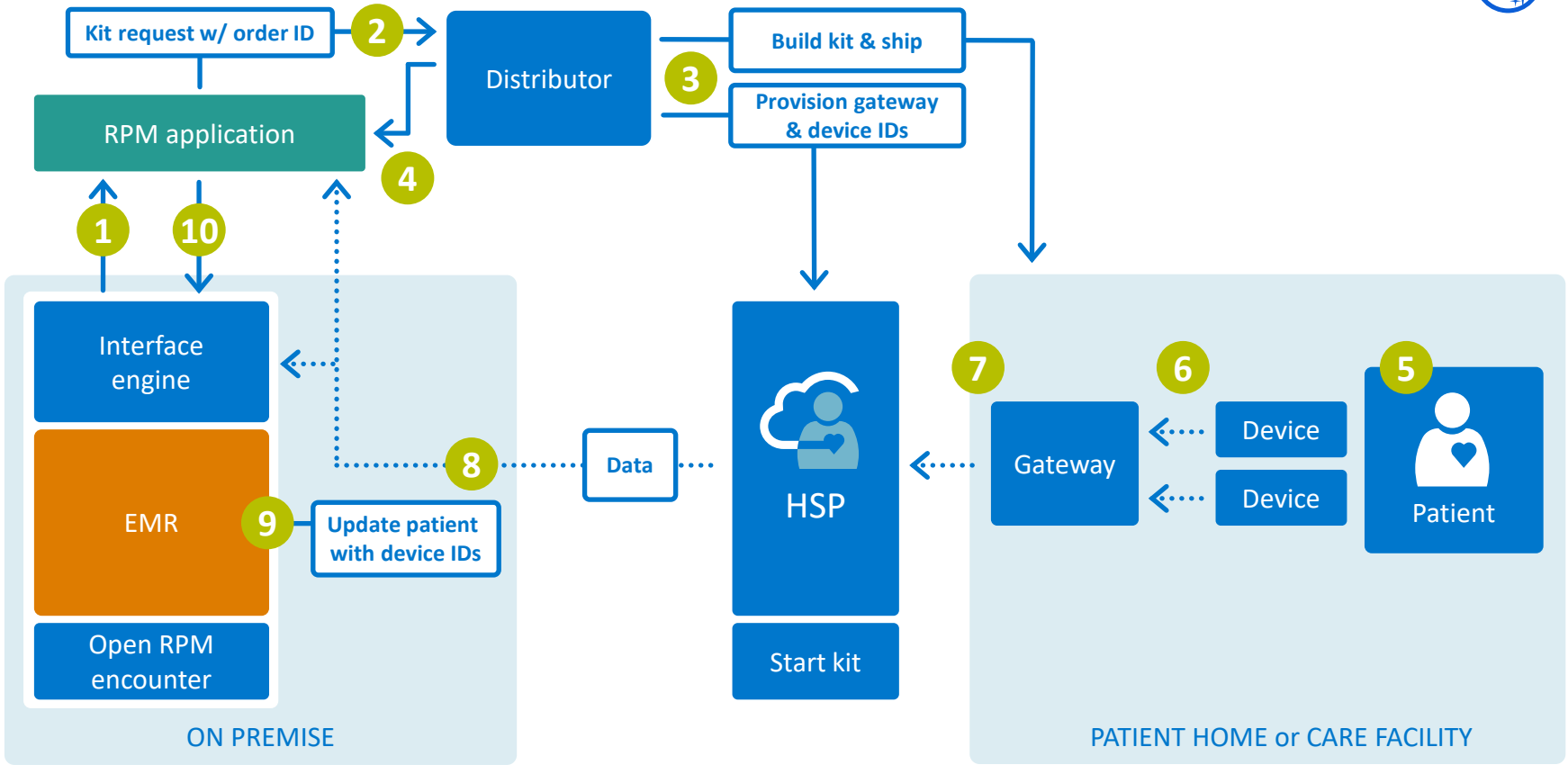
OPTION A EMR as ordering and monitoring application. Provisioned via Distributor.



OPTION A EMR as ordering and monitoring application. Provisioned via Distributor.

1. Hospital or clinic sends kit request to Distributor manually or via API / HL7 Order
2. Distributor provisions devices and gateway – ships to patient or facility to distribute
3. Distributor sends Gateway / Device ID to Interface Engine, then to EMR
4. End user takes reading on device(s)
5. Device sends reading to HealthSuite Gateway
6. Gateway sends reading to HealthSuite Platform (cloud)
7. Platform sends reading to Interface Engine
8. Interface Engine sends data to EMR
9. EMR links data to correct patient and provides monitoring capabilities

OPTION B RPM as ordering and monitoring application. Provisioned via Distributor.



OPTION B RPM as ordering and monitoring application. Provisioned via Distributor.

1. Hospital or clinic sends patient demographic information to RPM Application
2. RPM Application sends a kit request to Distributor manually or via API / HL7 Order
3. Distributor provisions devices and gateway – ships to patient or facility to distribute
4. Distributor sends Gateway / Device ID to RPM Application
5. End user takes reading on device(s)
6. Device sends reading to HealthSuite Gateway
7. Gateway sends reading to HealthSuite Platform (cloud)
8. Platform sends reading to Interface Engine and/or RPM Application
9. RPM Application links data to correct patient and provides monitoring capabilities
10. RPM Application sends either report or certain results to Interface Engine, then to EMR

Philips Cloud Strategy

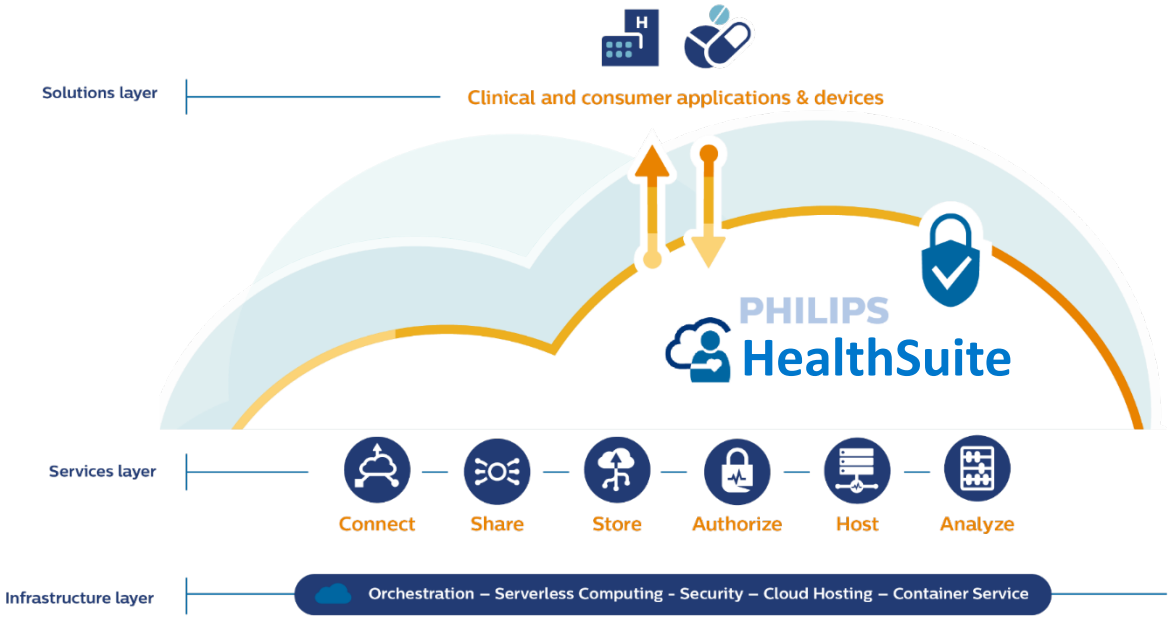
Philips Cloud strategy
Connecting the dots of patient data

Philips integrates personal health, vitals and clinical data to provide professionals and individuals with access to the actionable insights they need to deliver better health outcomes.

Philips HealthSuite Cloud

Cloud expertise and curated services to unlock data

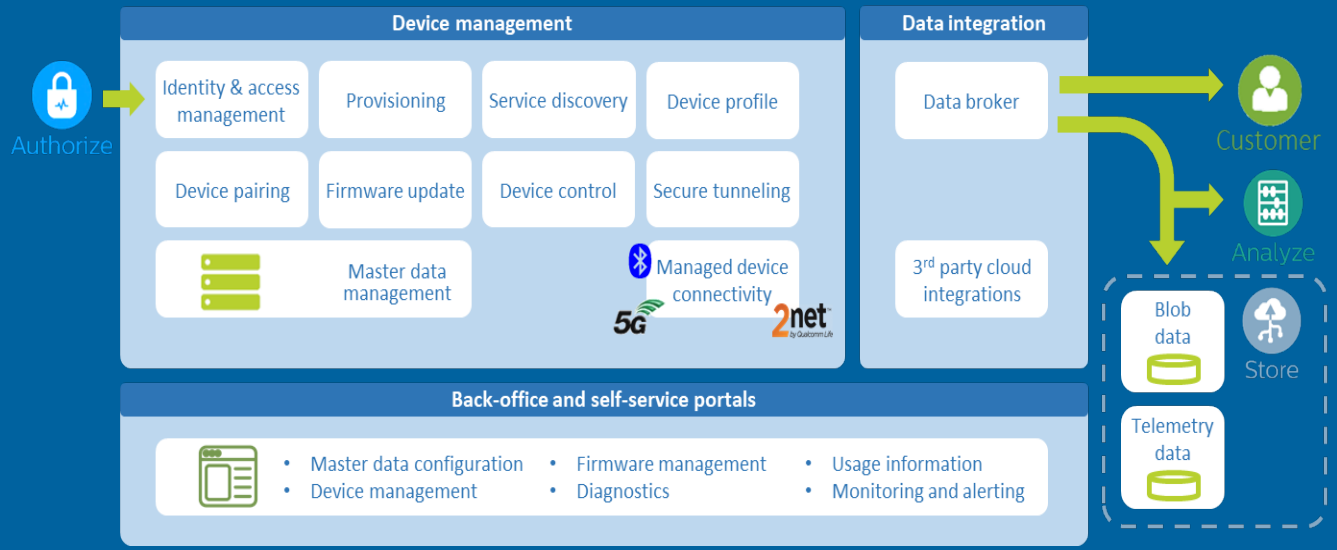
- **Orchestrated cloud infrastructure** with services to build and scale Healthcare solutions in the cloud
- **APIs** to aggregate clinical and consumer data and make data actionable with connected devices and data sources
- **Privacy, security and regulatory controls** to store & share data in a Healthcare compliant way
- Conformance to **Information Security** and **Quality Management System**
- **24 x 7 Operations Support** to configure, monitor and ensure operational availability



HealthSuite Connect

Connect

Manage, update, remotely monitor, and collect data from smart devices, ranging from consumer wearables to large medical-grade systems



Capabilities

- Master data management for propositions, applications, and devices
- Provision devices and apps with unique identities and keys ‘over-the-air’
- Dynamic discovery of platform services
- Store and retrieve device attributes & state
- Create and manage relationships
- Update firmware and software of devices
- Exchange events and messages
- Secure remote tunneling to devices
- Collect and broker data to HealthSuite or customer endpoints
- Store device data in various HealthSuite repositories
- Managed connectivity for (home) gateway- and peripheral devices
- Integration with 3rd party device clouds
- Self-service through client portals
- 24/7 monitoring and operational support
- Part of the larger HealthSuite platform ecosystem

Leading cloud expertise and regulatory compliant Cloud infrastructure

HSP meets the privacy, security, and regulatory requirements needed to protect an individual's sensitive data


PHILIPS