Clinical Insights Manager

Release 1.1 technical data sheet

The Philips Clinical Insights Manager (CIM) is a service-oriented end-to-end solution enabling high-resolution physiological and third-party bedside device data acquisition, access and archival.

Philips CIM features

- Captures and stores Patient Information Center iX (PIC iX) data for up to 1,024 beds at high resolution. A single CIM collector can capture data from multiple Primary Servers. CIM can capture data for up to 1,024 beds per collector. The 1,024 beds can be spread across multiple PIC iX servers.
- Stores patient monitoring physiological data from Philips bedside monitors, IntelliBridge bedside, IntelliBridge System, telemetry, and other Philips-approved devices in the Philips HealthSuite Platform. HealthSuite is powered by Amazon Web Services (AWS).
- Stores data in HealthSuite for 1 year.
- High-resolution data stores all captured data to meet future "big data" needs.
- Supports continuous capture of diagnostic quality (Dx) ECG for all patients monitored at the bedside. High resolution must be turned on at the bedside.
- CIM Data Analysis and Review includes two browser-based applications: **Clinical Insights Manager (CIM) Viewer** and **Alarm Insights Manager (AIM) Dashboard**.
- Data continuity: Data that fails to export to the HealthSuite cloud is stored in a local database. The data is forwarded once the connection is restored. For a 1,000 bed setup, CIM stores up to 6 hours of patient data locally, considering a 5-minute payload size of 1 GB.
  If connection to the cloud is not restored and maximum capacity of the store and forward is reached, the rest of the data is dropped.

Number of Beds	Downtime Stored Data (hours)
25	240
100	60
250	24
500	12
1,000	6

Stored data elements

CIM captures and stores the following data elements:

- Patient admission, discharge, and transfer (ADT) information including names, IDs, Bed, and demographics from the monitoring system. The ADT information can follow the patient in a continuous record as they move around the hospital.
- Alarms with available details, including event start time, alarm announce time, scrolling or escalating alarm text, and time that the alarm is acknowledged.
- Derived numeric parameters at 1-second intervals and aperiodic numerics such as NBP with detailed status of each parameter (current alarm limits, if the alarm is in progress). Parameters include complex numerics such as calculations and Early Warning Scores.
- CIM captures each beat-to-beat heart rate at one-half millisecond resolution for use in heart rate variability computations. This is a unique capability of CIM, beneficial to neonatal research.
- Raw, non-derived waveforms with a 24-waveform limit:
  - Stores default ECG waveforms at 250 samples per second (sps) and a monitoring bandwidth from 0.05 or 0.5 Hz to 20, 40, 55, or 125 Hz. Set the bandwidth at the patient bedside.
  - With the Diagnostic Quality option, stores ECG waveforms at 500 sps and a bandwidth from 0.05 to 150 Hz.
  - Stores a maximum of two limb leads with all chest leads. The other four limb leads can be mathematically computed.
- Arrhythmia monitoring information from the ST/AR algorithm describing current rhythms, location and classification of beats and pacemaker pulses, and a running signal quality measure.
- Alarms, numerics, and waves from IntelliBridge hubs and module-interfaced devices, such as ventilators, pumps, NIRS (near-infrared spectroscopy) cerebral oximetry.
- Detailed information about all source devices.
- Non-ECG waves (Pleth/SpO2, Pressure) are stored at the highest possible acquisition rate of 125 samples/s.
- Slow Moving waves (Resp) are stored at the highest possible acquisition rate of 62.5 samples/s.

Deployment

There are four elements to a successful CIM deployment:

- A virtual machine (VM) aggregates data from multiple PIC iX systems and sends the data to HealthSuite for storage and analysis.
- Installation and setup of CIM software on the VM.
- Configuration of PIC iX to export data to CIM.
- Onboarding users on HealthSuite for data access.

Clinical Insights Manager Viewer

CIM Viewer capabilities include:

- Authentication using HealthSuite Identity Access Management (IAM).
- Patient, time, and event-based navigation and visualization of data.
- Data export to standard formats: CSV for numeric and textual, and PhysioNet for waveforms and supporting metadata.
- User can export parameters, alarms, consolidate alarms, waves, and patient info in .zip format.
- An Open Data Access API allows programmatic access to data in CIM. Refer to the *Clinical Insights Manager Programming Guide* (part number 453665080531).

Alarm Insights Manager Dashboard

AIM Dashboard is a web-based application that provides insights into the overall alarm situation through an interactive and intuitive dashboard.

- Authentication using HealthSuite IAM.
- Identify actionable insights into hospital alarm system quality to eliminate noise, improve alarm accuracy, establish and share standards of care, provide sentinel event management.
- Build standard and ad-hoc alarm reports that can be automatically generated and shared across the enterprise.

Alarm Audit Log Migration (AALM) is a tool that provides a one-time migration of PIC iX Alarm Audit log (maximum 90 days) to Alarm Insights Manager (AIM). Once migrated, AIM can be used to explore and troubleshoot alarm issues. This migration is performed by Philips field services in tandem with R&D DevOps.

- Requires a license for AIM that covers the same clinical unit(s) as what will migrate from the PIC iX Clinical Audit Log.
- PIC iX must be version C.03 or higher.
- PIC iX language and regional settings must be one of the following supported locales:

Language	Regional Setting
en-US	English (US)
zh-CHN	Chinese (Simplified, China)
zh-TW	Chinese (Traditional, Taiwan)
cs-CZ	Czech (Czechia)
da-DK	Danish (Denmark)
nl-NL	Dutch (Netherlands)
fi-FI	Finnish (Finland)
fr-FR	French (France)
de-DE	German (Germany)
el-GK	Greek (Greece)
hu-HU	Hungarian (Hungary)
it-IT	Italian (Italy)
ja-JP	Japanese (Japan)
nb-NO	Norwegian Bokmål (Norway)
ro-RO	Romanian (Romania)
ru-RU	Russian (Russia)
es-ES	Spanish (Spain, International Sort)
pl-PL	Polish (Poland)
pt-BR	Portuguese (Brazil)
sv-SE	Swedish (Sweden)

Data Analysis & Review

CIM Data Analysis & Review capabilities include:
- Authentication using Philips HealthSuite- Identity Access Management (IAM).
- Patient, time, and event-based navigation and visualization of data.
- Data export to standard formats: CSV for numeric and textual, and PhysioNet for waves and supporting metadata.
- User can export parameters, alarms, consolidate alarms, waves, and patient info in ZIP format.
- Patient Data Auto Export - Multi Cloud Integration. The user has an option to schedule export jobs for a unit that runs on a predefined frequency. The scheduled job integrates with customer owned and managed cloud storage accounts. The following vendors are currently available for integration:
  - AWS S3
  - Azure Blob Storage
  - Google Cloud Storage

Security

Security by design

For details, refer to

http://www.usa.philips.com/healthcare/about/customer-support/product-security

Data security

- Data at rest on premise is encrypted using AES-256.
- All communication uses protocol TLS v1.2.
- All inbound communications to the application are via HTTPS only.

Application security

- HSDP OAuth uniquely authenticates each individual for access to web applications.
- For added security, multifactor authentication (MFA) is enabled for all user access to web applications.
- Each HTTPS request to HealthSuite requires a valid web token.
- A token is issued against an Identity Management Service (OAuth/IAM). Each application instance has an identity registered in HealthSuite.
- A token issued against the identity has a 30-minute validity after which the application must refresh the token.

Cloud security

- Internal microservices are displayed in a virtual private cloud within HealthSuite.
- API Gateway Architecture is implemented to prevent internal microservices from being publicly exposed via the Gateway service.
- All communication within cloud microservices is encrypted with HTTPS.

Operational security

- Application auditing and logging framework collects vulnerability, health and audit log analysis metrics to detect and alert on potentially suspicious activity.
- CIM and its components are monitored for new vulnerabilities. These are assessed and recommendations and/or updates are issued as needed.
- Security-related software updates that require customer action are communicated to customers through Philips InCenter.

Data Warehouse Connect migration

Philips supports migration of DWC version C.03+ data to CIM in HealthSuite through tools that Philips personnel execute and validate.

System Health Monitoring

The CIM cloud infrastructure is monitored 24x7 by the HealthSuite operations team. This includes monitoring database uptime and AWS services.

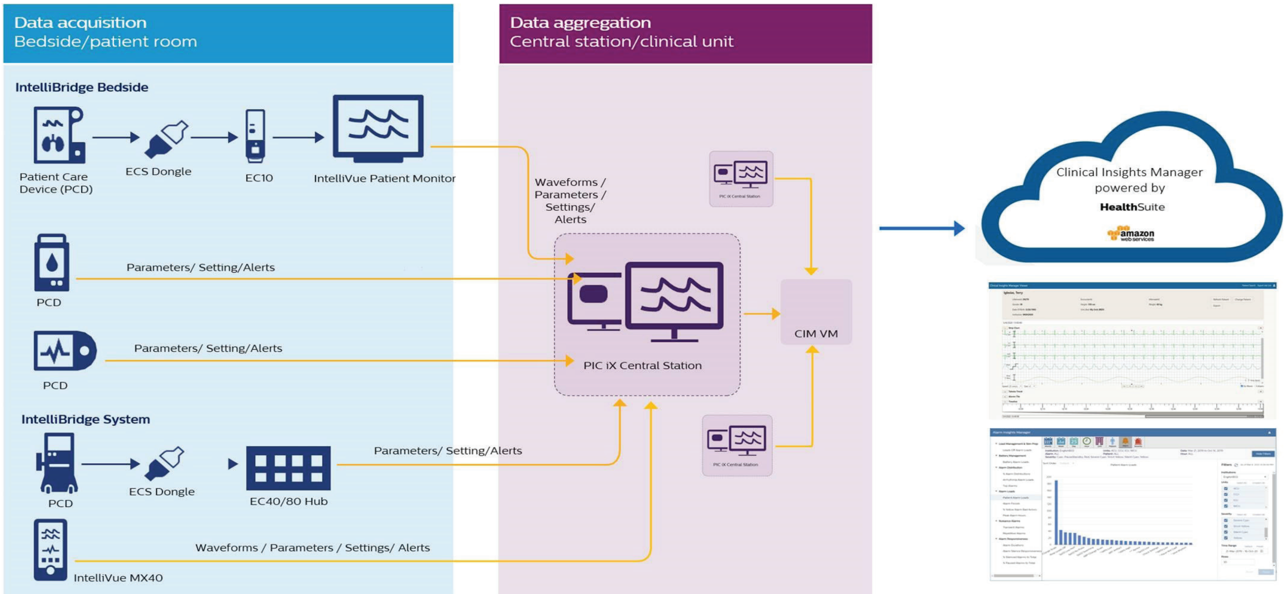
The CIM application suite and data store are monitored and maintained by a dedicated DevOps team. Monitoring includes:

Proactive monitoring and support

- Built-in watchdog services continuously monitor bottlenecks, sluggishness, or unexpected shutdown of core solution services and applications and send alerts to the DevOps team via email and dedicated Microsoft Teams channels.
- The DevOps team resolves these alerts before they become problems.

Reactive diagnostics and support

- A suite of application dashboards monitors events in the logs, performance counters for applications and services and provide a holistic view of system health.
- Kibana provides a consolidated view of all logs from different sources of the application suite. Kibana shows the issue and any notable surrounding events.



Privacy

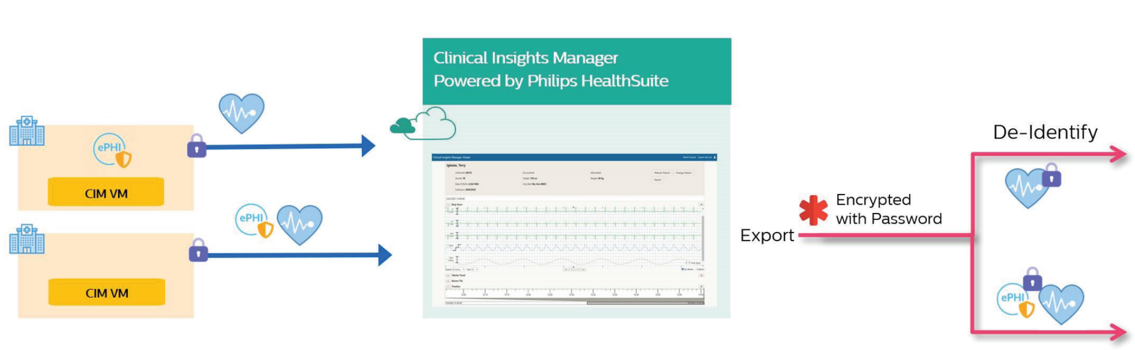
The Global Privacy Team completes a Privacy Impact Assessment to assure that no personal data is processed for secondary purposes.

CIM provides two configuration options to ease privacy concerns:

- Send ePHI information to HealthSuite. All ePHI information is encrypted using TLS v1.2 certificates over HTTPS. ePHI information is encrypted in flight and at rest in HealthSuite.
- Do not send ePHI information to HealthSuite. No ePHI information is sent to HealthSuite; only bed and unit labels are sent. The CIM Viewer application displays the patient by bed and clinical unit only. The AIM Dashboard is not affected since it does not have ePHI-related views.

Privacy for data export

For data export, CIM provides a configuration option to automatde-identify ePHI information. If the user chooses to de-identify before data export, CIM removes all ePHI information. Only unidentified data is exported. In addition, a password field is provided to encrypt the exported data files.



On-Premise VM specifications

For proper operation of the CIM software, the on-premise VM must be dedicated and not shared with other software. The following table lists the hardware specifications based on the CIM licensed product options.

Requested Data	Bed Range	RAM	Virtual CPUs	Speed (GHz)	Disk Size (SSD)	Network Upload Bandwidth	Payload
Alarms Only	<512	16 GB	4 vCPUs	2.2	172 GB	10 Mbps	<= 3 MB
Alarms Only	512–1,024	32 GB	6 vCPUs	2.2	172 GB	10 Mbps	<= 6 MB
All Data (Waves+Numerics+ Alarms+Events)	<512	32 GB	4 vCPUs	2.2	172 GB	50 Mbps	<= 1 GB
All Data (Waves+Numerics+ Alarms+Events)	512–1,024	64 GB	10 vCPUs	2.2	172 GB	100 Mbps	<= 2 GB

Firewall: On-Premise Customer-Provided Windows Virtual Machines

- Windows Firewall is enabled for all network profiles.
- The following ports and applications are exclusions for all network profiles on all hosts (inbound).
  - Remote Desktop (TCP 3389), NetBIOS (UDP 137, 138), SMB (TCP 445), DNS (UDP 53)
  - Microsoft .NET framework and WCF are open, regardless of license (TCP 8050, 8051, and 9912)
  - Windows Time (UDP 123)
  - HTTPS (TCP 443)
- Incoming data is allowed for Philips.ACP.ServiceHost.exe (UDP and TCP).

Virtualization software

Software	Version	Operating System
VMware ESXi	6.5, 6.7, 7.0	Windows Server 2019 or higher
Microsoft Hyper-V Server	2019	Windows Server 2019 or higher
Nutanix AHV	5.10.4 or higher	Windows Server 2019 or higher

Antivirus support

Philips tested and verified the following antivirus software for use with CIM. The customer can install other third-party antivirus software. The customer is responsible for ensuring the antivirus software does not interfere with the product's intended use.

- McAfee 10.6.1

Browser support

CIM supports the following web browsers:

- Google Chrome version 80 and higher
- Microsoft Edge version 80 and higher

Philips product compatibility

CIM is compatible with the PIC iX C.03 and 4.0 (and all associated IntelliVue MX, MP, MX40, and VSS series monitors).

Screen resolution

Full 1280 x 1080 or Higher at 100% scale or lower.

Third-party software

The following software is required and installed with CIM.

Software	Version
PostgreSQL	14
VC++ 2013 Redistributable Package	X64
.Net Framework	4.8
Postman	v8.0.10
Fiddler	v5.0.20204
Wireshark	v2.4.5

Note: The customer is responsible for applying security updates to all third-party software, OS, and VMware. Philips does not validate the security updates because CIM is not classified as a medical product.

4522 991 83021 * AUG 2023

How to reach us:

www.healthcare.philips.com

healthcare@philips.com