MEMORI

Configuration Guide

Altera EHR Integration

Sanome (Human Digital Twin Ltd)

Version 1.0

Below you will find a guide for the steps which need to be completed to integrate MEMORI into your hospital's Altera EHR. Installation shall be done by the customer's technical/IT team, with this guide and support provided by the manufacturer.

Software version

This configuration guide is applicable with the following devices:

- 20260415_infection-risk-predictor
- 20260415_user-helper
- 20260415_model-helper
- 20260415_ehr-connector

Table of Contents

Before configuration

Before starting the configuration, the manufacturer and customer IT team should agree on the items listed in Steps 1 and 2 below. In addition, Sanome will provide:

- URL of the MEMORI instance (e.g. prod.[hospital_name].sanome.net)
- The Next Best Actions form that has been signed off by the deployment site

The instructions in this configuration guide should be implemented in a staging or test (UAT) environment initially to allow for sufficient testing.

Step 0: Pre-requisites

The device runs on infrastructure and in a network managed by the manufacturer. The requirements are as follows:

- The device must be run on infrastructure and in a network managed by the manufacturer (managed via infrastructure-as-code tooling) so that it can be easily maintained and deployed.
- The manufacturer will ensure that any infrastructure that runs the device is specifically reserved for this purpose to avoid interference with other processes.
- The manufacturer will ensure that there are robust virus scans on all virtual machines.
- The device must be managed by the manufacturer (via an orchestration tool) so that the device can be easily stopped, started or updated as required.
- The infrastructure running the device must have at least 4 CPUs and 16 GB of RAM.
- This infrastructure must be able to run containerised workloads (to avoid risk of bugs caused by inconsistent deployment environments).
- The infrastructure containing patient data needs to be isolated via a custom virtual network.

There are no security options for the device that are set by the customer at installation time. All security requirements are pre-configured by the manufacturer before deployment. All installation requirements and restrictions are laid out in the steps below.

Step 1: EHR Data Egress

1.1 Secure network connectivity

A secure connection must be established between the hospital's EHR network and the manufacturer's network to enable the transfer of patient data. This may be achieved by:

- Establishing a site-to-site VPN between the two networks, or
- Configuring encryption in transit (e.g. mutual TLS) over an agreed network path.

Where an integration engine (e.g. Rhapsody, InterSystems HealthShare) sits between the EHR and the manufacturer's network, the same security requirements apply to each hop in the data path. The customer's IT team should verify that firewalls and network security groups are configured to allow only the necessary traffic between the networks.

1.2 Agree data transfer format and triggers

The manufacturer and the customer's IT team must agree on the following prior to configuration:

Data format	FHIR R4 is the preferred format. HL7v2 or proprietary formats may be supported by agreement.
Endpoints	The manufacturer will provide the endpoint URL to which data should be pushed.
Data types	The specific clinical data types to be sent (e.g. observations, demographics, encounters, medications). To be agreed during implementation planning.
Triggers	The events that should trigger data transmission (e.g. new observation set recorded, admission, discharge). To be agreed during implementation planning.
Integration engine	If an integration engine is used, the customer's IT team is responsible for ensuring data is correctly routed from the EHR to the manufacturer's endpoint.

1.3 Security considerations

The manufacturer's device will leverage the customer's existing security measures to ensure that data flow operates securely. The customer's IT team is responsible for ensuring that appropriate protections against malware are in place within the network, including the use of firewalls, anti-malware software, and other necessary security protocols. The manufacturer will work with the customer's IT team to ensure these security measures are compatible with the device's operational requirements.

The following hazardous situations result from a failure of the customer's IT network to provide characteristics required for the running of the device (these are listed in the manufacturer's risk management file):

- The user lacks information regarding the patient's health state.
- Unintended people have access to confidential patient data.

The manufacturer will monitor data ingestion to ensure continuity of data flow. Any disruption in data transmission will trigger an alert to the manufacturer to ensure timely investigation.

Step 2: EHR Data Ingress

The MEMORI risk score must be pushed back to the Altera EHR so that it is visible to clinicians. In addition to the risk category, associated metadata (e.g. observation set ID, timestamp, patient ID) will be included in the payload.

2.1 Agree score delivery format

The manufacturer and the customer's IT team must agree on the following:

Data format	The format in which the score will be pushed back to the EHR (e.g. FHIR Observation resource, HL7v2 ORU message). To be agreed during implementation planning.
Endpoint	The customer's IT team must provide the endpoint (or integration engine route) to which the manufacturer should push the score. The customer's IT team should ensure that this endpoint is appropriately scoped so that the manufacturer only has ability to push back the score and nothing else
Integration engine	If an integration engine is used between the manufacturer and the EHR, the hospital's IT team must ensure that the score data is correctly routed through to the EHR and ultimately appears in the patient record.

2.2 Monitoring

The manufacturer will monitor the score delivery pipeline and will be alerted to any downtime or delivery failures to ensure continuity of data flow.

Step 3: EHR Front-end Configuration

The following front-end configuration steps must be completed within the Altera EHR by the customer's IT team to surface the MEMORI score to clinicians.

Below are the high-levels steps needed to configure Altera front-end so that it can display MEMORI

3.1 Add MEMORI score to the flowsheet

The MEMORI score should be added as a row or field within the patient flowsheet (the same flowsheet that supports NEWS2) so that it is visible alongside other clinical observations.

3.2 Add MEMORI score to the tracker board

The MEMORI score should be added as a column on the tracker board (ward board) so that clinicians can see the score at a glance for all patients on the ward.

The column should be configured such these MEMORI scores display as the following colours:

- 'No Score' as not coloured
- 'Low' as green
- 'Moderate' as yellow
- 'High' as orange
- 'Critical' as red

3.3 Add MEMORI score to the patient list

The MEMORI score should be added to the patient list view so that it is visible when browsing patients.

3.4 Add MEMORI tab to patient context

A MEMORI tab should be added to the patient context within Altera. This tab should contain an embedded link to the patient-specific MEMORI explainability dashboard.

The hospital should configure this Altera tab so that different user groups have the correct permissions (the default being that all clinical users have access, no non-clinical users have access).

The dashboard URL follows this format:

prod.[hospital_name].sanome.net/dashboard/patients/[patient_id]

The [hospital_name] component will be provided by the manufacturer. The [patient_id] component should be dynamically populated with the patient's identifier from the EHR context.

Step 4: SSO Configuration

The manufacturer will provide the following parameters ahead of the application being set up:

- Redirect URI — for example, https://oauth.[hospital_name].sanome.net/oauth2/callback
- Scope: openid

The customer's IT team member with administrator access to the hospital's identity provider will conduct the following steps:

1. Register the Application: Set up an application in the hospital's identity provider using the OAuth2 authentication method. The redirect URI and scope should be entered as provided by the manufacturer. A client ID and client secret should be generated as part of the registration process.
2. Share Details: The client ID and client secret should be shared with the manufacturer.

Step 5: Device Deployment

Once the above steps have been completed, the manufacturer should set up the infrastructure (using infrastructure-as-code tooling) and then deploy the device using the orchestration management tool.

The manufacturer will conduct initial testing in a UAT environment to verify that:

- Data is flowing correctly from the EHR to the manufacturer's infrastructure.
- MEMORI scores are being generated and pushed back to the EHR as expected.
- The MEMORI dashboard is accessible and displays patient data correctly.
- SSO authentication is functioning.

If required, the manufacturer will conduct initial local calibration of the device prior to first use.

Step 6: Testing

The manufacturer and the customer's IT team should agree on a testing script prior to go-live. The testing script should cover the following areas:

6.1 Data flow and score generation

- Confirm that clinical data entered in the EHR reaches the manufacturer's infrastructure.
- Confirm that MEMORI scores are generated and returned to the EHR within the agreed timeframe.
- Validate that a variety of different MEMORI scores are correctly generated and displayed (Low, Moderate, High, Critical).

6.2 Partial observations

- Test behaviour when only a partial set of observations is available for a patient.
- Confirm that the system handles missing data gracefully and that the score reflects the available data.

6.3 Latency and timeliness

- Measure the end-to-end latency from observation entry in the EHR to MEMORI score appearing in the EHR.
- Confirm this is within the agreed acceptable timeframe.

6.4 Trigger and event testing

- Confirm that agreed trigger events (e.g. new observation set, admission) correctly initiate data transmission to the manufacturer.
- Confirm that the score is updated in the EHR following each trigger.

6.5 User roles and access control

- Confirm that SSO authentication is working correctly.
- Confirm that only users in the designated groups can access the MEMORI explainability dashboard.
- Confirm that the MEMORI score is visible in the flowsheet, tracker board, patient list, and patient context tab to the appropriate user roles.

6.6 MEMORI dashboard

- For a test patient, click through to the MEMORI explainability dashboard from the EHR and confirm the score matches that displayed in the EHR.
- Confirm that all graphs and patient data are correctly displayed on the dashboard.

Step 7: Maintenance & Decommissioning

No ongoing maintenance is required by the customer for the device to function as intended.

If the device requires an update that would impact this configuration, the manufacturer will contact the customer to provide details and any necessary steps to complete the update.

The manufacturer maintains logs and visibility of the version of the device in use by the customer.

If a security event is detected (such as a virus on one of the virtual machines running the device), the software will continue to run as normal. In this event, the manufacturer will be alerted via their monitoring system and will take appropriate steps, keeping the relevant stakeholders at the hospital informed.

Ensure that any changes to the EHR configuration — including upgrades, renaming fields, modifying observation types, or altering data structures — are communicated to Sanome. These changes can break the MEMORI integration silently, so advance notice is essential to prevent data flow or score delivery failures. Likewise, any disruption in data flow must be escalated via standard incident reporting pathways.

Decommissioning, if or when relevant, will be managed by the manufacturer. If any steps are required to be completed by the customer, the manufacturer will provide clear guidance.

Intended Use Statement

MEMORI is a modular software as a medical device (SaMD) which may utilize compatible software to obtain patient data collated from Electronic Health Record systems (EHR) and deliver a risk score (Memori Risk Score) to inform clinical management through the use of a proprietary Machine Learning model to categorise and stratify the risk of patients developing hospital acquired infections (HAIs) and predicting a set time frame of onset in the patient population. The MEMORI score and the information displayed on the explanatory dashboard can be used by a clinician to inform the management of a patient. Potential next actions may be displayed based on national guidelines and/or local policies as appropriate.

MEMORI is intended for use by trained healthcare professionals, including doctors, nurses, and healthcare assistants, for adult patients aged over 18 and under 90 years with acute neurological injuries and/or neurological conditions.

It is to be used within secondary care settings, including but not limited to:

- Acute brain injury wards
- Stroke units
- Complex neuro-rehabilitation units
- Prolonged Disorders of Consciousness (PDOC) units
- Ventilation and complex respiratory wards
- Neuro-behavioural wards
- Neurosurgical intensive care units (Neuro SICU)
- Intermediate neurological wards
- Neurological stepdown units

Use is restricted to the specified patient population and the defined clinical environments such as the above.

MEMORI is viewed on the care facility IT system through the EHR provider. Data from patients entered in the EHR, both physiological and non-physiological, is processed by the MEMORI algorithm and the generated risk score is displayed to clinicians via the EHR or MEMORI explainability dashboard. As patient data is updated with more monitoring inputs, the risk score is updated and displayed.

MEMORI is designed to predict the onset of HAIs and subsequently INFORM the clinician of this, to allow them to consider further investigations. This timely detection will translate into a clinician considering an appropriate intervention, thereby significantly reducing the risk of complications and shortening the extra length of stay usually associated with the development of HAIs. Where sufficient data is NOT available from the EHR, MEMORI will not provide a risk score to ensure only accurate information is displayed.

MEMORI is **NOT** intended to replace clinicians or multi-disciplinary team members, drive clinical management, be used in replacement of new observations, investigations or treatment decisions, be used as the sole driver for discharge of patients from the hospital, or to replace local or national guidelines.

Appendix: Version History

Version	Description	Date
v1.0	Initial version of Altera Configuration Guide	13/04/2026