Tool 1: Basic set of requirements for a (distributed) medical alarm infrastructure

Reading guide:
This tool can be used to create a basic set of requirements when replacing (components in) the medical alarm system.
There are two categories of recommendations: strongly advised' and 'may be considered', HCP=Heatlhcare Professional

Requirements for the full medical alarm system		
Category	**Strongly advised for all alarm system scenarios**	**May be considered, depending on care scenario and alarm system**
Application	• The entire medical alarm system should be reliable, accurate and have a high availability. • Verify the intended use of the alarm system. If it is used for medical alarm purposes in a critical care environment, the system should be considered a medical device and comply with this legislation. • Define the maximum allowable downtime during maintenance and software upgrades of (components in) the system. • The performance of the medical alarm system shoul be continuously monitored. In the event of a system failure the HCP should be informed directly. • A dashboard should be available to provide department specific overviews of alarm load, alarm recovery and escalation times as well as the distribution of different alarm categories per time interval (hour, day or week).	• Assigning responsibility for alarms from a patient to a HCP is simple and configurable per unit. The assignment should be secured to prevent unauthorized changes. • Alarms should always reach a HCP. If there is no response to an alarm, the system should support automatic escalation to a second HCP. • The medical alarm system must allow local preferences to be configured, such as filtering specific alarms, defining distribution rules, and setting escalation timeframes to a second HCP if an alarm by the first HCP remains unaddressed. • The system must support confirmation of alarm receipt (two-way communication in the medical alarm system) – ensuring acknowledgement that the alarm has been successfully delivered to the correct destination. • Alarms received on a mobile device should generate an acoustic signal, that can preferably be customized based on the urgency of the alarm. • The maximum "transmission" time from source of the alarm to the receiving mobile device must be specified, ideally with has a maximum delay of 10 seconds after alarm occurrence, unless a delay has been configured intentionally by the user. • An emergency procedure and possibly a backup system (e.g. light signals in the unit) may be required to mitigate risks in the event of a system failure. • The medical alarm infrastructure may be made more redundant by using a secondary transmission system alongside WiFi, such as 4G.

Legislation and standards	• The medical alarm system (or its components) is certified as medical device with the appropriate risk classification aligned with its intended use. • The medical alarm system must comply with data security and privacy requirements, as well as associated legislation and standards (e.g. in Europe: GDPR, NEN7510)	• The system and all components comply with relevant standards (like IEC, IHE PCD and IEC 80001). It is advised to require interoperability, preferably compliant with IEEE 11073 SDC interoperability standards.
Technical	• A simple and logical alarm infrastructure is required. • Where possible, components in the medical alarm system should be designed to allow another component to take over the task in the event of a failure. • Critical components in the medical alarm system should be designed to withstand power failures, e.g. by incorporating a backup battery power supply to maintain operation duting power interruption. • The system should support performance monitoring to check the proper functioning of all components in the medical alarm system. It is recommended to periodically review the performance of the system with special attention to vulnerable parts of the system, such as connections between components. • A maintenance plan must be established for the entire medical alarm system and its individual components, fitting the hospital's ICT infrastructure. • Inquire about the expected lifespan of the software as it typically differs from the technical lifespan of medical equipment.	• A development,test- and acceptance environment is used to test software updates before they are implemented in the clinic. • Adequate management of software updates is necessary to ensure optimal security with minimal downtime. Preferably, software upgrades should be centrally coordinated. • If hospital servers or Vmware are used, the company should specify the requirements of servers and database clusters.

Medical device as primary source for monitoring of physiological parameters (e.g. patient monitor, telemetry, CTG)		
Category	**Strongly advised for all alarm system scenarios**	**May be considered, depending on care scenario and alarm system**
Application	• The intended use should be to monitor physiological parameters • The medical device should be suitable for the intended patient population • The medical device should be reliable and measure accurately for its intended clinical application. • It should be possible to set upper and lower limits for each alarm type • The urgency of an alarm should be clearly indicated (e.g. using colors, red for critical and yellow for less critical alarms). • The alarm should be clearly visible, compliant with NEN-EN-IEC 60601—1-8/A1 and must include an auditory component. • The medical device should be designed for use in a medical alarm system, enabling the transfer of alarm type, alarm value and alarm priority within the system.	• It should be possible to set alarm limits for different (patient) profiles. • There should be an option to filter and delay the issuing of alarms, per department or per profile with central adjustment by administrators. • Administrators should be able to centrally adjust which alarms are sent to the medical alarm system. • Alarms shoud be send with context information (e.g. vital parameters, alarm priority, alarm text, room/bed number, device). • The system should support inter-bed communicatio, allowing alarms from other patient's monitors to be viewed if needed by the HCP. • Monitoring of vital parameters remains available on the bedside in the event of a power failure • It should be s possible to suppress or pause an alarm at the bedside. • It should be possible to remotely suppress an alarm. • The medical device is integrated in such a way that its alarms can be silenced if it is connected to the medical alarm system. • It should be possible to add alarms from other medical equipment via the patient monitor, to the alarm system.
Technical	• Central logging of all alarms is supported. The log files are accessible to both the service technicians and the users.	

Central monitoring station / central collection of signals		
Category	**Strongly advised for all alarm system scenarios**	**May be considered, depending on care scenario and alarm system**
Application	• The intended use should state that the application is monitoring physiological parameters. • The central monitoring station should be designed for flexible set up and should include an overview screen displaying patients, their current measured values and active alarms. • It should be clearly indicated which alarms are active and for each patient. • The central monitoring station should provide visible and -if possible- audible singals to indicate a broken connection between the bedside monitor and the central station.	• At the central monitoring station it should be possible to create an overview of alarms for each patient but also of the entire unit over a selected period. It is possible to search for alarms. • It should be possible to suppress or pause alarms directly at the central monitoring station. • At the central monitoring station it should be possible to transfer patients to another department. • The central monitoring station should display the most important parameters of the connected equipment with minimal delay
Technical	• The central monitoring station has a bi-directional connection to each bedside monitor allowing bi-directional interaction.	• The central monitoring station preferably has a bi-directional connection with other connected equipment, allowing for interaction, such as remote adjustment of alarm limits or initiating a blood pressure measurement.

Other medical devices in the medical alarm system		
Category	**Strongly advised for all alarm system scenarios**	**May be considered, depending on care scenario and alarm system**
Application	• An alarm can be transmitted through an output port and transferred to a medical alarm system. • The manual clearly defines which messages are categorized as alarms and which are notifications. In addition, the assigned alarm priority level (high, medium, low, informative) must be stated.	• The medical device is integrated with the medical alarm system in such a way that the forwarded alarm can be considered a primary alarm in the medical alarm system. • The medical device is connected such that its alarms can be silenced when integrated with the medical alarm system. • The ability to remotely silence alarms on the medical device (e.g. the mobile device receiving the alarms) may be a desirable feature.
Technical	• Logging of all alarms is possible. These log files are accessible to service technicians as well as to users.	• Alarms can be sent to the HCP with contextual information (e.g. room, type of alarm, bed number, device). The standard used for transmitting this information must be specified (e.g. HL7, IHE, FHIR or SDC). • The medical device must be capable of transmitting both data and alarms to different recipients (e.g. sending alarms to the (medical) alarm system and data to the Electronic Medical Record (EMR)).

Central server solution for collection alarms and/or alarm distribution		
Category	**Strongly advised for all alarm system scenarios**	**May be considered, depending on care scenario and alarm system**
Application	• The server solution is capable to handle various types of alarms from different sources and processing them appropriately (filtering and forwarding). • The server solution has sufficient capacity to handle all alarms and ensure reliable data storage. • The server solution must forward all alarms to the mobile devices in accordance with the configured settings.	• The software should support configuring filtering, grouping and delaying of alarms before forwarding them within the system. Adjusting the priority of a distributed alarm according to medical use should be possible. • Continuous logging of alarms and their processing should be performed with sufficient detail and options for retrospective analysis, down to the level of the individual HCP. • The system should support generating alarm reports at department level, enabling for alarm or workflow optimization tailored to each department. • If the system processes full disclosure data, it should also support the creation of trend reports at parameter level.
Technical	• The server solution should offer high reliability and availability • The server solution should be equipped with an automatic switching mechanism to ensure communcation is taken over without interruption by another component in case a communication port fails. • The system should generate a notification when the connection is broken or lost • All ICT components should comply with security standards, such as NEN7510. • The server solution should be easy to maintain and allow for remote monitoring. • The server should provide timely alerts when the maximum capacity limits for processor, memory or storage are approaching. • Release notes for new software versions should be provided to the hospital before new updates are implemented.	• Servers in the medical alarm system should be designed such that in the event of a failure, another server component can take over the task • The server hardware should preferably run in a central server environment where critical factors such as emergency power supply, network provision and climatic conditions are centrally managed. • The server solution should be integrable with a performance monitoring system, allowing performance monitoring up to the service and application level • The local ICT organization should be able to perform virus scans and security checks on the server. • Backup and snapshots should be tailored to the needs of the system.

Network and WiFi		
Category	**Strongly advised for all alarm system scenarios**	**May be considered, depending on care scenario and alarm system**
Application	• In case of failure of network or WiFi, it is possible to display alarms on an overview screen/ central monitoring station.	• It should be visible and/or audible to users if the network or WiFi is not functioning, indicating that the alarm system is broken and that an emergency procedure must be initiated by the HCP.
Technical	• The network and WiFi should be assessed by the supplier of the medical alarm system to ensure compatibility and to define specifications for reliable deployment of the system in the WiFi network. • The network and WiFi should have a high reliability and availability, with the maximum allowable downtime clearly defined. • The network and WiFi should be adequately secured in accordance with applicable standards, such as the NEN7510. • The network and WiFi should provide sufficient coverage to ensure continuous data transfer towards on mobile devices.	• The maintenance intervals of network or WiFi should be coordinated with the departments that use the medical alarm system. • Investigate whether there are possibilities to use another network as a backup in addition to WiFi, for example 4G.

Mobile device - hardware		
Category	**Strongly advised for all alarm system scenarios**	**May be considered, depending on care scenario and alarm system**
Application	• The mobile device should be reliable, robust and suitable for use in a medical workflow. • The mobile device should support the software and/or apps that are required to receive alarms from all medical alarm systems used in the department. • The mobile device should have appropriate display(s) and buttons for managing alarms effectively. • The mobile device should be easy to clean and meet the requirements of the hygiene department's standards. • The mobile device should be operated by the HCP while wearing medical gloves.	• The mobile device itself may qualify as a medical device, but it is not mandatory. However, the handling software on the mobile device should classify as a medical device. • The mobile device should enable users to generate emergency calls such as an assistance request or an employee safety alert. • The mobile device should be easy to charge for instance by using a "charging rack"). • The battery should be easy to replace, ideally without interruption of the alarm system. • The device should support night mode, allowing for dimming of light and sound. • Sound and vibration settings, including individual alarm configurations and minimum sound levels can be managed centrally and are adjustable at the department level. • Consideration should be given to whether the option to mute the sound on the device is permittedin accordance withrelevant standards.
Technical	• Logging should be available on the mobile device and on the specific Apps for the users.	• Mobile device management can be configured on the device to allow immediate roll out of security updates. • The device should be set up to be unusable for the alarm system outside the hospital. The device does not contain any local data and if the device is lost, all medical information and apps will be deleted.

Mobile device - software		
Category	**Strongly advised for all alarm system scenarios**	**May be considered, depending on care scenario and alarm system**
Application	• The software for alarm handling is a medical device. The intended use of the software should specify the transmission of alarms. • The alarm should be clearly visible in the software including information on which patient and/or bed location the alarm was generated. • Alarms should be immediately readable on the mobile device without requiring any user actions. • The recent history of alarms should be accessible on the mobile device. • The medical software should be user-friendly, with a clear and understandable display alarms. • The software should notify users if the (WiFi) connection with the alarm system is interrupted. • The design should be such that logging out does not lead to any dangerous disruptions in thealarm system. • An alarm should be generated on the devices (at department level) if a room has not been assigned to a device in the software.	• The software should display alarm type and priority. If possible, ringtones and volume levels should be adjusted for specific alarms. • It should be possible to manage alarms or forward them to a colleague (buddy-HCP). • The screen should show the current valuesof at least two important vital parameters (e.g. heart rate, saturation) depending on the scenario and device. • The software should allow users to easily view patient's alarm history. • It should provide access to trends or a live display of parameter curves from the monitor. The option to temporarily assign or refer to a colleague via the app may be desirable, e.g. when the HCP is occupied with caretaking and unableto manage alarms from anotherpatient.
Technical		• If the alarm information is distributed with the patient name, it is advised to use personal login to the mobile device.

Tool 2: Process guide for using medical alarm systems safely

Reading guide:

This tool consists of a set of policy and process steps that a hospital can adopt when implementing a medical alarm system. It is designed to assist users and engineers in defining procedures for safe use of the medical alarm system. Processes intended for system users are highlighted in green, while those for service organizations and technical departments are shown in blue.

The recommendations are categorized into 'strongly advised' and 'may be considered',

Policy/Process	Strongly advised:	May be considered, depending on local situation:
Policy for **patient monitoring and alarms**	• Establish a clear policy on the use of monitoring and the neccesary equipment, either at department or hospital-wide. • Identify the departments, patient groups, and indications for which monitoring will be used. • Define the required type of equipment for each application and specify the corresponding alarm system. • Define criteria for determining when a patient no longer requires monitoring. • Create information for patient and their relatives about the medical devices and the purpose of alarms. Address potential concerns they may have and incorporate their feedback in the development of the information materials. • Implement a hospital-wide training policy to ensure all users are properly educated. • Review the hospital policy every two years, evaluate the policy to confirm its relevance and ensure the existing alarm system still meets the functional requirements.	• Consider forming a multidisciplinary team to establish a hospital policy on monitoring and alarm management. • Incorporate guidelines from scientific associations to determine which patient group should be monitored, specifying parameters and monitoring frequency. • Evaluate the need for a department specific policy to address their local needs. • Implement a process for periodic analysis and evaluation of the number of alarms to optimize the effectiveness and usability of the alarm system.

Application of alarm systems **1: alarm assignment and handling**	• Define who is authorized to set alarms and alarm limits and specify the circumstances under which these settings may be adjusted. Consider implementing predefined profiles for different patient categories to streamline alarm setup. • Define who is responsible for handling alarms, e.g. consider having one first responsible for alarm handling with a buddy who can take over the alarm handling if the primary HCP is occupied.	• Consider implementing a delay in the transfer of alarms to a buddy HCP. The acceptable time period between the occurrence of an alarm and its handling can be customized per department. However, if hospital-wide settings are required due to technical constraints, a multidisciplinary team should be responsible for the policy and time configurations in the medical alarm system. • Define practical alarm handling rules within the team, such as guidelines for adjusting or pausing alarms and specifying who is authorized to perform these actions and at which location. Ensure patient and their relatives are also informed about the handling procedures, thereby reassuring them that all alarms are seen and managed by an HCP even though the HCP is not physically present at the bedside. • Recognize that alarms in an alarm system can lead to alarm fatigue. Periodically evaluate and optimize alarm settings, but also alarm transfer settings and delays in the medical alarm system. Modern systems often include dashboards that monitor and display alarm statistics to assist in optimization.
Application of alarm systems **2: dealing with disruptions in the alarm system**	• Ensure that users can always determine whether the medical alarm system is functioning properly. For example, consider implementing visual or auditory signal to alert users to a failure in one or more components or an interruption of the alarm system. • Establish an emergency procedure to be followed in the event of a system failure, specifying how the patient's monitoring should be managed at this time. Ensure all healthcare providers in the department are informed about this emergency procedure. • Determine a procedure for using the assistance/emergency button if a colleague needs help with a patient. Ensure that all HCPs in the department are aware of this procedure. • Report disruptions in the system to the correct technical department within the hospital (e.g. ICT or engineering). Define which technical department is responsible to solve problems with components in the medical alarm system (define a service level agreement) • Develop a procedure for informing the patient and their relatives about faults or emergencies in the medical alarm system, ensuring clear communication during such incidents.	• Implement periodic refresher courses for users of the medical alarm system, which also covers the emergency procedure to ensure preparedness for critical situations. • Establish a process for evaluating significant system errors and define risk mitigating measures for the future.

Application of alarm systems **3: risk - assessment**	• Conduct a risk assessment of the processes involved in using the alarm system. This should be carried out by a multidisciplinary team of users and clinical engineers, considering the complete workflow of alarm handling. Ensure that risk mitigation measures are known to users. • Perform a technical risk assessment for all components in the medical alarm infrastructure. Risk mitigating measures for the identified technical risks should be implemented during the medical alarm system's implementation phase.	• Request input from the company/supplier, as they have conducted their own (often confidential) risk assessment of the technical system. This information can provide valuable insights for the risk analysis. • Discuss residual risks with the users, for instance during training sessions.

Application of alarm systems 4: **checks after maintenance and upgrades**	• Ensure that both a technical check (conducted by clinical engineers) and a functional check (conducted by users) are completed before implementing a medical alarm system.
	• A functional test plan must be available for users to execute. The technical service organization must have a technical test plan.
	• A functional check must also performed after maintenance/upgrade/major failures in the system before going live again.
	• Establish clear agreements between the different technical departments within a hospital.
	• The technical departments must have a procedure on maintaining the system and infrastructure. This procedure should include: a plan for performing upgrades and maintenance and a robust communication strategy to inform HCP's about maintenance schedules and planned upgrades.
		• Ensure adequate documentation of all tests:
		  ○ the functional test plan should be reviewed, approved and stored
		  ○ technical test plan should be reviewed, approved and stored
		  ○ all failures in the system are adequately logged and tracked.
		• Implement a system to handle requests for changes in the medical alarm system, to ensure central assessment (e.g. on impact in the ICT environment)
		• If artificial intelligence is incorporated for decision support in the alarm system, establish a specific policy for maintenance, validation and testing. This policy should align with the national guideline for AI in healthcare.

training	• Develop an adequate training program for users of the medical alarm systems. The progam should include: the initial training for new users as well as a plan for periodic retraining, specifying its form and frequency. • Update the training program if the design or processes of alarm management are changed	• Aspects to consider in training program: how to configure and set alarms, methods for handling alarms and emergency procedures. • Actively involve clinical engineers and technical departments (medical technology, application support) in developing the technical aspects of the training. • Consider organizing discussion sessions to address locally experienced challenges and discuss potential improvements to the alarm system and its operation.
Information about the **alarm system**	• Ensure that all medical equipment and all ICT components in the medical alarm architecture are inventoried and documented (including software version). Consider to describe - Information on which equipment & software versions are used - how components are interconnected - differences in terms of configuration or usage between the different department • The service organization should implement a system for continuously monitoring the alarm system to ensure it is operational and running correctly ("chain monitoring of the alarm infrastructure") • If the use of the alarm system is intended for a medical purpose, it is considered a medical device and should comply with the applicable legislation. In the EU compliance with the MDR is required. A risk class IIb is recommended when the system monitors critical vital parameters.	• Document the entire alarm architecture in a central reference document, including details about all system components and the locations where the alarm settings can be accessed. • Maintain alarm log files for a short period to facilitate analysis of alarm handling failures. • Pay special attention to the connection between components to ensure the correct transmission of alarm and/or information.
Responsibilities by the **service organization**	• Ensure that responsibilities for each component of the alarm system are explicitly defined, especially when multiple technical service departments are involved in maintaining (parts of) the alarm system.	• It is preferable to have one central service desk to coordinate actions in the event of malfunctions. This service desk should be well-known and accessible to all users.

Procedure **for technical testing, acceptance and release**	• Provide a technical test procedure, test plan and/or checklist to be utilized both after system acceptance and following maintenance. • Define who is responsible for performing tests upon acceptance, after updates, after upgrades, following malfunctions and after routine maintenance.	• Record all technical tests performed and make these accessible to users (e.g. in an equipment management system) • Establish a dedicated test environment for critical alarm systems to test and simulate. This environment can be used to validate system updates, changes and new implementations before they go live.
procedure for technicians how to deal with system failure	• Ensure a clear procedure is established for handling system failures, including: a description of how technical service departments should respond to faults in the alarm system (both during and outside office hours) and guidelines for effective communication to the affected clinical departments.	• Implement a power supply with no-break or emergency power for critical components in the alarm system in case of power failure. • Implement critical components redundantly to reduce the risk of complete system failure. • Develop a manual for technicians addressing common malfunctions in the system in order to reduce the time needed for problem solving.
investment plan	• Develop an investment plan to ensure sufficient budget is available over the years for the replacement of (components in) the alarm system	-