Digistat® Care
Manuale Utente

Versione 22.0

10/27/2025

Ascom UMS s.r.l. Unipersonale
Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italy
Tel. (+39) 055 0512161 – Fax (+39) 055 829030
www.ascom.com

Digistat® Care versione 2.5

Digistat® Care è prodotto da ASCOM UMS s.r.l. (http://www.ascom.com).

Il prodotto ASCOM UMS Digistat® Care ha la marcatura CE 2460 ai sensi del Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio del 5 aprile 2017 (MDR).

ASCOM UMS è certificata conforme alla norma EN ISO 13485:2016 per "*Product and Specification development, marketing, sales, production, installation and servicing of information, communication and workflow solutions for healthcare including software and integration with medical devices and patient related information systems. Marketing, sales and installation of information, communication and workflow solutions for healthcare including hardware and software.*"

Licenza software
Digistat® Care deve essere utilizzato solo dopo aver ottenuto una licenza valida da Ascom UMS o dal Distributore

Licenze e marchi registrati
Digistat® è un Marchio Registrato di ASCOM UMS s.r.l. Tutti gli altri Marchi Registrati sono dei rispettivi possessori.
In questo documento, ovunque siano menzionati, Android™, Google™ e Google Play™ sono da considerarsi marchi di Google, LLC; iOS, Apple® e App Store® sono da considerarsi marchi di Apple.

Sommario

1. Uso del Manuale

Questo manuale utente deve essere utilizzato in combinazione con i manuali specifici dei singoli moduli, elencati di seguito. Fare riferimento ai manuali applicabili, in base ai moduli Digistat Care in uso nell'Organizzazione ospedaliera.

USR ITA Controlbar
USR ITA Controlbar Web
USR ITA Smart Central
USR ITA Fluid Balance
USR ITA Fluid Balance Web
USR ITA Infusion
USR ITA Patient Explorer
USR ITA Patient Explorer Web
USR ITA Scoring Calculator
USR ITA Smart Monitor
USR ITA Smart Monitor Web
USR ITA Therapy
USR ITA Therapy Web
USR ITA MDI Web
USR ITA Vitals Web
USR ITA Smart Central Mobile
USR ITA BCMA (Mobile)
USR ITA Vitals Mobile
USR ITA Mobile Launcher
USR ITA CDSS Configurator Mobile
USR ITA Digistat Gateway
USR ITA multiAssist module

1.1 Intenti

Il presente manuale fornisce tutte le informazioni necessarie per garantire un utilizzo sicuro di Digistat Care e per consentire di identificarne il fabbricante. Vuole inoltre essere una guida di riferimento per l'utente che desideri sapere "come fare" a compiere una determinata operazione, nonché una guida al corretto uso di Digistat Care affinché possano essere evitati usi impropri e potenzialmente pericolosi.

1.2 Caratteri usati e terminologia

L'uso di Digistat Care richiede una conoscenza di base dei più comuni termini e concetti informatici. Allo stesso modo, la comprensione del presente manuale è subordinata a tale conoscenza.
Inoltre, l'utilizzo di Digistat Care deve essere consentito soltanto a personale professionalmente qualificato ed opportunamente addestrato, con l'eccezione di utenti non professionisti per funzionalità specifiche (tale eccezione è eventualmente specificata nelle istruzioni d'uso).
I riferimenti incrociati interni al documento funzionano, nel caso si stia consultando la versione on-line del manuale, come collegamenti ipertestuali. Ciò significa che ogni volta che si trova il riferimento a una immagine ("Fig 2", ad esempio) o a un paragrafo ("paragrafo 2.2.1", ad esempio) è possibile cliccare sul riferimento per accedere direttamente a quella particolare figura o a quel particolare paragrafo.

I dati di natura clinica che vengono mostrati nelle immagini presenti in questo manuale sono esempi creati artificialmente in un ambiente di test, e il loro unico scopo è quello di spiegare la struttura e le procedure di Digistat Care. Non sono dati reali presi da procedure cliniche effettive, e non devono essere considerati come tali.

Le parti relative alle specifiche configurazioni di Digistat Care sono in inglese all'interno del manuale. Tali configurazioni dipendono dalle procedure effettive adottate dall'organizzazione ospedaliera che usa Digistat Care e saranno in seguito implementate nella lingua richiesta dall'organizzazione ospedaliera.

1.3 Convenzioni

Nel documento sono utilizzate le seguenti convenzioni:

- I nomi dei pulsanti, le voci dei menu, le opzioni, le icone, i campi e qualunque cosa nell'interfaccia possa essere utilizzato dall'utente (tramite tocco o click o selezione) sono formattate in **grassetto**.
- I nomi/titoli delle schermate, delle finestre e delle "tabs" sono citate "Fra virgolette".
- Il codice di programmazione è formattato in carattere Courier.
- Il simbolo ➢ indica un'azione che l'utente può effettuare per portare a termine una certa procedura.
- I riferimenti a documenti esterni sono formattati in *corsivo*.

1.4 Simbologia

Nel manuale sono utilizzati i seguenti simboli.

Informazioni utili

Questo simbolo appare in corrispondenza di informazioni aggiuntive riguardanti le caratteristiche e l'uso di Digistat Care. Si può trattare di esempi esplicativi, di procedure alternative o di qualsiasi informazione "a lato" si ritenga utile ad una più approfondita comprensione del prodotto.

Attenzione!

Questo simbolo è usato per evidenziare informazioni volte a prevenire un uso improprio del software o per sottolineare procedure critiche che potrebbero portare a situazioni rischiose. È perciò necessario prestare estrema attenzione ogni volta che il simbolo appare.

I seguenti simboli sono usati nel box informativo (About Box):

Indica nome e indirizzo del fabbricante

Attenzione, consultare la documentazione allegata

Indica all'utente di consultare le istruzioni d'uso allo scopo di ottenere importanti informazioni cautelative quali avvisi o precauzioni che non possono essere presentate sul dispositivo medico stesso per varie ragioni.

1.5 La Digistat Suite - Sguardo d'insieme

La Digistat Suite è un PDMS (sistema di gestione dei dati-paziente) modulare teso a creare soluzioni che possano soddisfare le necessità relative la gestione dei dati-paziente. Le diverse soluzioni sono create abilitando i moduli richiesti, facenti parte dei due prodotti della suite, che sono:

- Digistat Docs (che non è un dispositivo medico);
- Digistat Care (che è un dispositivo medico di classe IIb in UE, in accordo all'MDR).

Digistat Docs è un software che registra, trasferisce, immagazzina, organizza e mostra informazioni e dati relativi ai pazienti allo scopo di supportare il personale clinico nella creazione di una cartella clinica elettronica.
Digistat Docs non è un dispositivo medico.

Digistat Care è un software che gestisce informazioni del paziente e dati relativi al paziente, inclusi dati e eventi provenienti da sistemi e dispositivi medici, e fornisce informazioni a supporto di trattamento, diagnosi, prevenzione, monitoraggio, predizione, prognosi e mitigazione della malattia.
Digistat Care è un dispositivo medico di classe IIb in UE, in accordo all'MDR.

Entrambi i prodotti sono modulari, perciò l'organizzazione ospedaliera può scegliere se abilitare tutti i moduli disponibili oppure abilitarne solo una parte, a seconda delle proprie esigenze e dei propri scopi.

I moduli possono essere aggiunti in tempi diversi. La suite di software può quindi cambiare nel tempo, in accordo ai possibili cambiamenti nei bisogni dell'organizzazione. In questi casi viene fornito un addestramento aggiuntivo e la configurazione è nuovamente validata con il coinvolgimento dell'organizzazione ospedaliera.

1.6 Informazioni sulla Digistat Suite

Il pulsante **Info** sul menu principale permette di visualizzare una finestra contenente informazioni sulla versione installata della Digistat Suite, sui prodotti e sulle relative licenze (About Box).

L'etichettatura del prodotto è l'About Box visualizzato sulle postazioni di lavoro client e sui dispositivi mobili sui quali è installata la Digistat Suite.

In conformità con il regolamento di esecuzione (UE) 2021/2226 della commissione del 14 dicembre 2021, le istruzioni per l'uso sono fornite in formato elettronico. L'About Box del prodotto contiene l'indirizzo web dove è possibile scaricare l'ultima versione delle istruzioni per l'uso.

2. Digistat Care

Digistat Care è un sistema di gestione dei dati dei pazienti ed un sistema di allarme in grado di implementare un set di varie funzionalità.

Digistat Care permette di visualizzare cruscotti per il monitoraggio del paziente in tempo quasi reale, di aggiungere nuovi parametri acquisiti nel sistema, di calcolare nuovi parametri derivati (ad esempio Severity Scores o CDSS).

Digistat Care si integra con dispositivi medici selezionati (ad esempio pompe di infusione, monitor-paziente, ventilatore, macchina per dialisi ecc.) per visualizzare, su pc fissi o su specifici smartphones, una notifica secondaria di eventi per il personale clinico.

Digistat Care può mostrare dati sia da dispositivi destinati ad essere usati in un sistema di allarmi distribuito affidabile ("reliable distributed alarm system") sia da dispositivi destinati ad essere usati in un sistema informativo distribuito (non "reliable")

Digistat Care è progettato per fornire una visione d'insieme dello stato del dispositivo, mettendo in evidenza allarmi e/o notifiche che si verifichino su un determinato dispositivo collegato, in modo che l'utente, con uno sguardo, possa essere informato della situazione del reparto.

Oltre a ciò, Digistat Care introduce il supporto agli "wearables", dispositivi indossabili dal paziente. Digistat Care inoltre fornisce informazione aggiuntiva al personale clinico, quale il calcolo degli Score (anche in combinazione con gli "wearables") e supporto alla decisione clinica (ad esempio il calcolo automatico del bilancio idrico, l'interazione fra farmaci o la notifica delle allergie del paziente.

2.1 Destinazione d'uso

Digistat Care è un software che trasferisce, immagazzina, elabora, aggrega, organizza e visualizza informazioni del paziente e dati relativi al paziente, inclusi dati e eventi provenienti da sistemi e dispositivi medici, così come informazioni inserite manualmente, al fine di indirizzare la gestione clinica, fornendo informazioni per:

- Supportare il trattamento, la diagnosi, la prevenzione, il monitoraggio, la predizione, la prognosi e la mitigazione delle malattie.
- Assegnare priorità o identificare segnali precoci di malattia o condizioni del paziente.

Digistat Care include:

- Raccolta di dati clinici e eventi dai dispositivi medici e dai sistemi in tempo quasi reale;
- Raccolta di dati inseriti dall'utente;
- Elaborazione/filtraggio configurabile per ottimizzare/ridurre la frequenza e il numero di notifiche di eventi al personale clinico allo scopo di presentare informazione clinicamente agibile;

- Visualizzazione di dati del paziente e di informazione sullo stato dei dispositivi in tempo quasi reale e retrospettivamente, al personale clinico su dispositivi di visualizzazione designati;
- Componenti di integrazione (Integrators) e comunicazione (Communicators) di un "distributed information system" (DIS) il cui scopo è quello di fornire al personale clinico notifiche di allarmi tecnici e fisiologici insieme a dati clinici e non clinici come supporto al monitoraggio dei pazienti;
- Componenti di integrazione (Integrators) e comunicazione (Communicators) di un "distributed alarm system" (DAS) il cui scopo è destinato a trasmettere e fornire in modo affidabile allarmi fisiologici e tecnici da dispositivi e sistemi sorgente selezionati agli operatori sanitari su dispositivi di visualizzazione designati e a specifici sistemi;
- Elaborazione di dati che fornisca informazione aggiuntiva al personale clinico, quali sistemi di calcolo degli score clinici e sistemi di supporto decisionale;
- Trasferimento dell'informazione acquisita a sistemi esterni clinici e non clinici in tempo quasi reale attraverso un'interfaccia, o retrospettivamente via query sui dati.

Digistat Care è un software stand-alone che è installato su un hardware specificato e si basa su uso e operatività appropriati dei dispositivi medici collegati, dei sistemi, dei dispositivi di visualizzazione e della rete IT dell'organizzazione ospedaliera.
Digistat Care opera insieme a Digistat Docs, l'altro prodotto della Digistat Suite;
Digistat Care è usato all'interno di strutture sanitarie in unità di terapia intensiva, sub-intensiva, unità non intensive e in altri reparti e, per funzioni limitate, nell'abitazione del paziente.
La popolazione di pazienti e le condizioni dei pazienti sono stabilite dai dispositivi e sistemi collegati e dalla specifica configurazione di Digistat Care richiesta dall'organizzazione ospedaliera che ne fa uso.
Gli utenti sono professionisti sanitari formati, ad eccezione degli utenti non professionisti per funzioni limitate.

Informazioni aggiuntive sulla destinazione d'uso:

- Il software supporta sistemi di scoring e un sistema di supporto alla decisione clinica, però non sono forniti di default né scores né algoritmi all'interno di tale sistema. Il software può effettuare calcoli in automatico solo dopo essere stato configurato in base alle decisioni degli utenti finali /clienti e dopo essere stato da essi validato.
- Il tipo di dati e di eventi clinici gestiti dal software dipende per lo più dalla sua configurazione: il software può trasferire, immagazzinare, elaborare, aggregare, organizzare e visualizzare dati e eventi clinici provenienti da input degli utenti o da qualsiasi altra fonte che abbia un output compatibile con il software e che sia stata opportunamente configurata in fase di installazione. Similmente, gli output del software, quali ad esempio il calcolo degli score menzionati sopra, o i dispositivi medici effettivamente connessi, dipendono dalla configurazione del software stesso.

2.2 Benefici per il paziente / Dichiarazioni

Il Prodotto:

- Riduce il numero di messaggi di allarme ricevuti dagli operatori sanitari, mirando così a ridurre l'affaticamento da allarme;
- I messaggi di allarme sono distribuiti in quasi tempo reale (near real-time), con l'obiettivo di ridurre i tempi di risposta degli operatori sanitari;
- I messaggi di allarme sono distribuiti in quasi tempo reale (near real-time), con l'obiettivo di supportare gli operatori sanitari nell'individuazione degli allarmi critici;
- Migliora l'efficienza del flusso di lavoro per il personale sanitario;
- Aiuta a organizzare la cura del paziente;
- Monitorando le infusioni aiuta a mantenere la continuità dell'infusione, che è un aspetto importante per la sicurezza del paziente;
- Raccoglie automaticamente i dati del paziente, con l'obiettivo di ridurre gli errori di trascrizione.

2.3 Uso “Off-label” di Digistat Care

Ogni uso di Digistat Care (da qui in avanti: il Prodotto) al di fuori di quanto indicato nella Destinazione d’uso (usualmente chiamato uso “off-label”) è sotto la completa discrezionalità e responsabilità dell’utente e della organizzazione ospedaliera. Il produttore non garantisce in nessuna forma la sicurezza e la adeguatezza allo scopo del Prodotto quando esso viene usato al di fuori di quanto indicato nella Destinazione d’uso.

2.4 Popolazione dei pazienti

Il Prodotto è destinato ad essere usato in collegamento con dispositivi e sistemi medici e la popolazione dei pazienti è da questi determinate. Il prodotto ha i seguenti limiti tecnici:

- Il peso del paziente deve essere compreso fra 0.1kg e 250kg
- L’altezza del paziente deve essere compresa fra 15cm e 250cm

2.5 Gruppi di utenti

I gruppi di utenti del prodotto sono definiti come segue: “*Utenti che Reagiscono agli Allarmi, Personale Infermieristico, Personale Medico, Utenti Tecnici e Pazienti*”.
Gli Utenti che Reagiscono agli Allarmi sono gli utenti primari; essi comprendono il Medico (Medical Doctor), l'Infermiere Professionale (Registered Nurse), l’Operatore Socio Sanitario/Assistente infermiere (Nurse Assistant), l'Infermiere Caposala (Charge Nurse) e l'Infermiere con formazione complementare (Nurse Practitioner). Questi utenti possono visualizzare e agire sugli avvisi gestiti dal Prodotto.
Il gruppo degli Infermieri comprende l'Infermiere Professionale (Registered Nurse), l’Operatore Socio Sanitario/Assistente infermiere (Nurse Assistant), l'Infermiere Caposala (Charge Nurse) e l'Infermiere con formazione complementare (Nurse Practitioner); insieme ai Medici, esso gestisce i dati dei pazienti nel Prodotto al fine di supportare la cura del paziente. Cioè, ad esempio, aggiorna la cartella clinica del paziente, monitora e registra i parametri vitali, definisce e documenta il piano di trattamento, ecc.

Il gruppo Utenti tecnici è legato solo all'installazione e alla configurazione del sistema. Gli Utenti Tecnici sono utenti secondari che includono il Tecnico di Assistenza, il Tecnico di Assistenza sul Campo, l'Ingegnere di Supporto Tecnico, l'Ingegnere Biomedico e l'Istruttore Tecnico.
I pazienti sono utenti solo per limitate funzioni del prodotto: tali funzioni però non costituiscono in alcun modo indicazioni sulla diagnosi o sul trattamento. In queste funzioni limitate, il paziente può inserire manualmente le misurazioni dei parametri vitali e può visualizzare i parametri vitali acquisiti automaticamente dai dispositivi medici di terze parti collegati (es. dispositivi indossabili).

2.6 Avvertenze per la sicurezza

L'Utente dovrà basare le decisioni e gli interventi terapeutici e diagnostici solamente a partire dalla verifica diretta della fonte primaria di informazioni. È esclusiva responsabilità dell'Utente la verifica della correttezza dell'informazione fornita dal Prodotto, nonché l'uso appropriato della stessa.
Solo le stampe firmate digitalmente o su carta da medici professionisti autorizzati devono essere considerate valide come documentazione clinica. Nel firmare le suddette stampe, l'Utente certifica di aver verificato la correttezza e la completezza dei dati presenti sul documento.
Nell'inserire dati relativi al paziente l'Utente ha la responsabilità di verificare che l'identità del paziente, il reparto/unità dell'organizzazione ospedaliera e il letto visualizzati sul Prodotto siano corretti. Questa verifica è di importanza fondamentale in caso di operazioni critiche quali, ad esempio, la somministrazione di farmaci.
L'organizzazione ospedaliera ha la responsabilità di identificare e implementare procedure appropriate per assicurare che i potenziali errori che si verificano sul Prodotto e/o nell'uso del Prodotto siano rilevati e corretti velocemente e che non costituiscano un rischio per il paziente o l'operatore. Queste procedure dipendono dalla configurazione del Prodotto e dalle modalità d'uso scelte dall'organizzazione ospedaliera.
Il Prodotto può fornire, a seconda della configurazione, accesso ad informazioni sui farmaci. L'organizzazione ospedaliera ha la responsabilità di verificare, all'inizio e poi periodicamente, che questa informazione sia corretta e aggiornata.
Per utilizzare il Prodotto in ambiente clinico, tutti i componenti del sistema – di cui il Prodotto fa parte – devono soddisfare tutti i requisiti normativi applicabili.
Qualora a seguito della fornitura elettrica venga a costituirsi un "sistema elettromedicale", attraverso il collegamento elettrico e funzionale con i dispositivi medici, rimangono a carico dell'organizzazione ospedaliera la verifica di sicurezza elettrica e il collaudo del sistema elettromedicale risultante, anche nel caso in cui Ascom UMS abbia effettuato in tutto o in parte i collegamenti necessari.
Nel caso che alcuni dei dispositivi in uso per il Prodotto si trovino all'interno dell'area paziente o siano collegati ad attrezzature che si trovano all'interno dell'area paziente, l'organizzazione ospedaliera ha la responsabilità di assicurarsi che tutto l'insieme sia conforme alla norma internazionale IEC 60601-1 e a qualsiasi altro requisito determinato dalla legislazione locale.
Il Prodotto è un software stand-alone che opera su comuni computer e dispositivi mobili collegati alla rete locale dell'organizzazione ospedaliera. L'organizzazione ospedaliera è responsabile di proteggere adeguatamente computer, dispositivi e rete locale contro cyber-attacchi o altri malfunzionamenti.

Il Prodotto deve essere installato solo su computer e dispositivi che soddisfano i requisiti hardware minimi e solo sui sistemi operativi supportati.
L'uso del Prodotto deve essere consentito, attraverso apposita configurazione degli account degli utenti e attraverso la sorveglianza attiva, soltanto ad Utenti 1) addestrati secondo le indicazioni del Prodotto da personale autorizzato dal produttore o dai suoi distributori, e 2) professionalmente qualificati ad interpretare correttamente le informazioni da esso fornite, ed a implementare le procedure di sicurezza opportune.
L'organizzazione ospedaliera è responsabile della definizione di un piano di "disaster recovery"; le pratiche adeguate includono, ma non sono limitate a questo, la continuità del business e le politiche di backup dei dati.

Digistat Suite fornisce una soluzione che può supportare l'organizzazione ospedaliera nell'implementazione di una politica di continuità del business. Si vedano le informazioni riguardanti il componente Export Scheduler nei manuali di installazione e configurazione.

2.7 Rischi residui

Un processo di gestione dei rischi è stato implementato nel ciclo di vita del Prodotto, così come prescritto dalle norme tecniche di rifermento. Per ogni rischio sono state individuate e implementate tutte le opportune misure di controllo che permettono di ridurre ogni rischio residuo a livello minimo che risulta accettabile considerando i vantaggi forniti dal prodotto. Anche il rischio residuo totale risulta accettabile se confrontato con i medesimi vantaggi.

I rischi sotto elencati sono stati affrontati e ridotti a livelli minimi. Tuttavia, per la natura stessa del concetto di rischio, non è possibile ridurli a zero ed è quindi necessario, secondo la normativa, portarne a gli utenti conoscenza.

- Impossibilità di utilizzare il Prodotto o alcune sue funzionalità come atteso, che può portare a ritardo o errore nelle azioni terapeutico/diagnostiche.
    - Un esempio di questo rischio è la mancata ricezione di un allarme da parte dell'utente (causata per esempio da una temporanea distrazione). Viene prodotta una notifica sonora per richiamare l'attenzione dell'utente e dunque ridurre tale rischio.
- Rallentamento delle performance del Prodotto, che potrebbe causare ritardi e/o errori nelle azioni terapeutico/diagnostiche.
- Azioni non autorizzate operate dagli utenti, che possono portare ad errori nelle azioni terapeutico/diagnostiche.
- Configurazione del Prodotto errata o incompleta, che potrebbe causare ritardi e/o errori nelle azioni terapeutico/diagnostiche.
- Attribuzione dell'informazione ad un paziente sbagliato (scambio di pazienti), che può portare ad errori nelle azioni terapeutico/diagnostiche.
- Errata gestione dei dati del paziente, incluso errori di visualizzazione, aggiunta, modifica e cancellazione dei dati che possono causare ritardi e/o errori nelle azioni terapeutiche/diagnostiche.

- Uso off label del Prodotto (ad esempio, il Prodotto è usato come Sistema primario di notifica di allarmi quando i dispositivi medici collegati non la supportano; decisioni e interventi diagnostico/terapeutici basati solamente sulle informazioni fornite dal Prodotto).
- Divulgazione non autorizzata di dati personali degli utenti e/o del paziente.

RISCHI RELATIVI ALLA PIATTAFORMA HARDWARE UTILIZZATA PER IL DISPOSITIVO MEDICO

- Shock elettrico per paziente e/o operatore, che può portare a lesioni o morte del paziente e/o dell'operatore.
- Surriscaldamento di componenti hardware, che possono portare a lesioni non gravi per il paziente e/o l'operatore.
- Contrazione di infezioni per paziente e/o operatore.

2.8 Responsabilità dell'organizzazione ospedaliera

Ascom UMS declina ogni responsabilità per le conseguenze sulla sicurezza ed efficienza del dispositivo determinate da interventi tecnici di riparazione o manutenzione non espletati da personale del proprio Servizio Tecnico o da Tecnici autorizzati da Ascom UMS.
Si richiama l'attenzione dell'utente e del responsabile legale dell'organizzazione ospedaliera in cui l'apparecchio viene utilizzato sulle responsabilità di loro competenza, alla luce della legislazione vigente in materia di sicurezza nei luoghi di lavoro e di Vigilanza sul campo per incidenti pericolosi o potenzialmente pericolosi.
Il Service di Ascom UMS è in grado di fornire ai clienti il supporto necessario a mantenere nel tempo la sicurezza ed efficienza delle apparecchiature fornite, garantendo la competenza, dotazione strumentale e le parti di ricambio adeguate a garantire nel tempo la piena rispondenza dei dispositivi alle originarie specifiche costruttive.

Il Prodotto è stato progettato prendendo in considerazione i requisiti e le "best practices" presenti nello standard IEC 80001 e nei suoi documenti tecnici correlati. In particolare lo IEC/TR 80001-2-5 ha grande rilevanza per il prodotto. Così come reso chiaro nella serie IEC 80001 parte delle attività necessarie e delle misure di controllo del rischio sono sotto il controllo e la responsabilità dell'organizzazione ospedaliera. Si faccia riferimento agli standard e ai documenti collegati al fine di identificare le attività necessarie e le misure di controllo del rischio; in particolare si faccia riferimento ai seguenti documenti:

- IEC 80001-1
- IEC/TR 80001-2-1
- IEC/TR 80001-2-2
- IEC/TR 80001-2-3
- IEC/TR 80001-2-4
- IEC/TR 80001-2-5

Il Prodotto non è progettato né offre funzionalità per la consultazione o la conservazione della documentazione prodotta.
I documenti generati tramite la suite sono prodotti dinamicamente sulla base dei dati e delle configurazioni disponibili al momento della loro creazione.
Di conseguenza, non è possibile garantire che le stampe successive mantengano il medesimo contenuto o formato delle versioni precedenti.
Si raccomanda di conservare una copia digitale ufficiale per eventuali necessità di verifica.

2.9 Responsabilità del fabbricante

Ascom UMS è responsabile agli effetti della sicurezza, affidabilità e delle prestazioni del prodotto soltanto se:

- l'uso e la manutenzione siano conformi a quanto indicato nella documentazione del Prodotto (che include il presente manuale d'uso);
- l'installazione e la configurazione sono eseguite da personale appositamente formato e autorizzato da Ascom UMS
- configurazioni, modifiche e manutenzione siano effettuate da personale formato ed espressamente autorizzato da Ascom UMS;
- l'ambiente nel quale il Prodotto venga utilizzato sia conforme alle prescrizioni di sicurezza e alle normative applicabili;
- l'ambiente nel quale il Prodotto venga utilizzato (inclusi computer, collegamenti elettrici, attrezzature) sia conforme alla normativa applicabile.

2.10 Rintracciabilità del Prodotto

Con lo scopo di assicurare la rintracciabilità del prodotto e azioni correttive sul posto, in conformità alle direttive EN 13485 e MDR 2017/745, all'acquirente è richiesto di informare ASCOM UMS o il suo Distributore riguardo qualunque trasferimento di proprietà mediante documentazione scritta attestante il Prodotto ed i dati identificativi del precedente proprietario ed il nuovo.
I dati del Prodotto possono essere trovati nell'etichetta del Prodotto (schermata "A proposito" mostrata all'interno del prodotto – si veda il paragrafo 1.6).
In caso di dubbi o domande a proposito dell'identificazione del Prodotto, per favore contatta l'assistenza tecnica d ASCOM UMS o del suo Distributore (per i contatti si veda il paragrafo 5).

2.11 Sistema di sorveglianza post-vendita

Il dispositivo marcato CE 2460 in accordo alla MDR è soggetto a sorveglianza post-vendita – che ASCOM UMS e il suo Distributore eseguono per ogni copia venduta – riguardo rischi potenziali ed attuali, sia per il paziente che per l'Utente, durante il ciclo di vita del Prodotto.

In caso di malfunzionamento o di deterioramento delle caratteristiche o del rendimento del Prodotto, inclusi gli errori d'uso dovuti a caratteristiche ergonomiche, così come qualsiasi

inadeguatezza nelle informazioni con esso fornite che possa avere costituito o possa costituire un rischio per la salute del paziente o dell'utente, o che possa costituire un rischio per la sicurezza dell'ambiente, l'Utente deve immediatamente dare notifica ad Ascom UMS o al suo distributore.

In caso di degradazione delle caratteristiche del Prodotto, prestazioni scadenti o istruzioni dell'utente inadeguate che possono o possono essere state un rischio per la salute del paziente o dell'Utente o per la sicurezza dell'ambiente, l'Utente deve immediatamente darne notifica ad ASCOM UMS o al suo Distributore.

Alla ricezione di un feedback da parte dell'Utente, oppure se rilevata internamente una tale necessità, ASCOM UMS o il suo Distributore avvieranno immediatamente il processo di verifica e revisione ed effettueranno le azioni correttive necessarie.

2.12 Vita del Prodotto

Il ciclo di vita del Prodotto non dipende dal logoramento o altri fattori che possono compromettere la sicurezza. Esso è influenzato dall'obsolescenza dei componenti dell'ambiente software (ad esempio OS, Framework .NET) ed è pertanto fissato a tre anni dalla data di rilascio della versione del Prodotto considerata (disponibile nella finestra "Informazioni").

3. Specifiche Software e Hardware

Il Prodotto deve essere installato esclusivamente da personale addestrato e autorizzato. Questo include il personale di Ascom UMS/Distributore e qualsiasi altra persona specificamente formata e esplicitamente autorizzata da Ascom UMS/Distributore. In mancanza di una esplicita, diretta autorizzazione da parte di Ascom UMS/Distributore, il personale dell'organizzazione ospedaliera non è autorizzato ad eseguire procedure di installazione o a modificare la configurazione del Prodotto.

Il Prodotto deve essere utilizzato solamente da personale addestrato. Il Prodotto non può essere utilizzato in mancanza di una appropriata formazione, effettuata dal personale di Ascom UMS/Distributore.

Le informazioni fornite in questa sezione coprono gli obblighi informativi a carico del produttore identificati dalla norma IEC 80001-1 (Application of risk management for IT-networks incorporating medical devices).
È responsabilità dell'organizzazione ospedaliera mantenere l'ambiente di esecuzione del Prodotto, inclusi l'hardware e il software, così come descritti in questo capitolo. La manutenzione include gli aggiornamenti, gli upgrades, le patches di sicurezza dei sistemi operativi, dei browser web, di Microsoft Framework .NET, di Adobe Reader, etc., così come l'adozione delle altre migliori pratiche per la manutenzione dei componenti hardware e software.

In base alla norma IEC 60601-1, per le stazioni di lavoro al posto letto, o che comunque sono posizionate in "Area Paziente", è necessario l'uso di dispositivi di grado medicale. Usualmente in questi luoghi vengono utilizzati PANEL PC di grado medicale. Se richiesto Ascom UMS può suggerire alcune possibili apparecchiature di questo tipo.

Un lettore PDF supportato deve essere installato sulle postazioni di lavoro al fine di visualizzare l'help on line. Si veda il paragrafo 3.1.3.

3.1 Posto letto e Centrale

3.1.1 Hardware

Requisiti hardware minimi:

- Processore x64 (ad esempio: Intel® I3)
- Memoria RAM 4 GB
- Hard Disk con almeno 60 GB di spazio libero
- Monitor 22'' con risoluzione 1920 x 1080 o superiore, con altoparlante integrato. Raccomandato touch screen.
- Mouse o altro dispositivo compatibile.
- Interfaccia Ethernet 100 Mb/s (o superiore)

Se una workstation Centrale / Posto Letto è configurata per visualizzare flussi video (funzione supportata solo in Smart Central con integrazione telecamera abilitata) i requisiti minimi sono i seguenti:

- Processore x64 (ad esempio: Intel® I3)
- Memoria: 4 GB di RAM + 50 MB per ogni stream video di una telecamera visualizzato contemporaneamente (ad esempio con 20 videocamere visualizzate 4 GB + 1 GB)
- Hard Disk con almeno 60 GB di spazio libero
- Monitor 22'' con risoluzione 1920 x 1080 o superiore, con altoparlante integrato. Raccomandato touch screen.
- Mouse o altro dispositivo compatibile.
- Interfaccia Ethernet 100 Mb/s (o superiore)

Alcuni esempi: con Intel i7 6600 2,60 Ghz, con uno streaming di 10 telecamere con un bitrate di 3138 kbps, l'utilizzo della CPU è circa del 45%. Con I3 7100t 3.4 Ghz, con uno streaming di 16 telecamere con un bitrate di 958 kbps, l'utilizzo della CPU è di circa il 30%.

3.1.2 Sistema Operativo

- Microsoft Corporation Windows 10
- Microsoft Corporation Windows 11

3.1.3 Software di sistema

- Microsoft .NET Framework v4.8
- Adobe Acrobat Reader versione 24

I manuali utente del Prodotto sono dei file in formato PDF generati in accordo alla versione standard PDF 1.5 ed è perciò leggibile da Adobe Acrobat 6.x o superiore. Inoltre, i manuali utente del Prodotto sono stati testati con Adobe Acrobat Reader 24. L'organizzazione ospedaliera può usare una differente versione di Acrobat Reader: la verifica del Prodotto installato include la verifica della corretta leggibilità dei manuali utente.

3.2 Server applicativo

3.2.1 Hardware

Requisiti hardware minimi (piccole installazioni, 20 letti, 4 dispositivi per letto):

- Processore x64 (ad esempio: Intel® I5) con quattro “core”.
- Memoria RAM 8 GB
- Hard Disk con almeno 120 GB di spazio libero
- Interfaccia Ethernet 100 Mb/s (o superiore). Raccomandato 1 GB.

Requisiti hardware raccomandati (installazione di medie dimensioni, 100 letti, 4 dispositivi per letto, Connect e Mobile):

- Processore x64 (ad esempio: Intel® I7) con otto “core”.
- Memoria RAM 32 GB
- Hard Disk con almeno 120 GB di spazio libero
- Interfaccia Ethernet 100 1 GB

3.2.2 Sistema Operativo

Deve essere installato uno dei seguenti sistemi operativi:

- Microsoft Corporation Windows Server 2016
- Microsoft Corporation Windows Server 2019
- Microsoft Corporation Windows Server 2022
- Microsoft Corporation Windows Server 2025

3.2.3 Software di sistema

- Microsoft Framework.NET 4.8
- Net Core Runtime & Hosting Bundle (per maggiori dettagli si veda il documeto INST ENG Digistat Web)

3.3 Server database

3.3.1 Hardware

Requisiti hardware minimi (piccole installazioni, 20 letti, 4 dispositivi per letto):

- Processore x64 (ad esempio: Intel® I5) con quattro “core”.
- Memoria RAM 8 GB
- Hard Disk con almeno 120 GB di spazio libero
- Interfaccia Ethernet 100 Mb/s (o superiore). Raccomandato 1 GB.

Requisiti hardware raccomandati (installazione di medie dimensioni, 100 letti, 4 dispositivi per letto, Connect e Mobile):

- Processore x64 (ad esempio: Intel® I7) con otto “core”.
- Memoria RAM 32 GB
- Hard Disk con almeno 120 GB di spazio libero
- Interfaccia Ethernet 100 1 GB

3.3.2 Sistema Operativo

Deve essere installato uno dei seguenti sistemi operativi:

- Microsoft Corporation Windows Server 2016
- Microsoft Corporation Windows Server 2019
- Microsoft Corporation Windows Server 2022
- Microsoft Corporation Windows Server 2025

3.3.3 Software di sistema

Deve essere installata una delle seguenti versioni di Microsoft SQL Server:

- Microsoft SQL Server 2016;
- Microsoft SQL Server 2017;
- Microsoft SQL Server 2019;
- Microsoft SQL Server 2022;
- Microsoft SQL Server 2022 Express.

3.4 Digistat Mobile

3.4.1 Android

Il Prodotto è compatibile con dispositivi Android dalla versione 5.1 alla versione 15.0. La compatibilità è stata verificata su dispositivi Myco 3 e Myco 4 (fino ad Android 14.0), Google Pixel 9a (Android 15.0) e iPhone 14.

L'applicazione è progettata per essere compatibile con altri dispositivi Android con una dimensione minima dello schermo di 3.5''; la compatibilità con ciascun dispositivo specifico deve quindi essere verificata prima dell'uso in ambito clinico.

I moduli Vitals Mobile, BCMA e CDSS Configurator Mobile di Digistat Mobile sono compatibili con dispositivi con Android 6.0+.

Dopo l'installazione di Digistat Mobile, prima dell'uso clinico, se i dispositivi scelti non sono quelli menzionati sopra, devono essere effettuate una verifica di compatibilità e una validazione, in accordo alla procedura descritta nel documento Digistat Mobile compatibilty checklist ACDM-585-12771 document.

3.4.2 iOS

Digistat Mobile è compatibile con dispositivi iOS. La compatibilità è stata verificata su dispositivo iPhone 14.
La compatibilità con un diverso dispositivo iOS deve essere verificata prima dell'uso clinico.

Dopo l'installazione di Digistat Mobile, prima dell'uso clinico, se i dispositivi scelti non sono iPhone 14, devono essere effettuate una verifica di compatibilità e una validazione, in accordo alla procedura descritta nel documento Digistat Mobile compatibilty checklist ACDM-585-12771.

3.5 Digistat Gateway

Digistat Gateway è compatibile con i dispositivi Android dalla versione 9.0 alla 15.0. La compatibilità è stata verificata su dispositivi Myco 3, Myco 4 (fino ad Android 14.0) e Google Pixel 9a (Android 15.0). L'applicazione è stata progettata per essere compatibile con i dispositivi Android con una dimensione minima dello schermo di 5''; la compatibilità con un dispositivo specifico deve essere verificata prima dell'uso clinico.
Per poter accedere alle funzionalità complete di Digistat Gateway è richiesta una SIM card con un piano voce. Inoltre, in caso di installazione senza connessione Wi-Fi in grado di garantire l'accesso al driver dell'applicazione Gateway, è richiesto un piano dati (la connessione di tipo LTE è fortemente consigliata).
Si prega di contattare Ascom UMS o il suo Distributore per la lista completa dei dispositivi che supportano Digistat Gateway.

Dopo l'installazione di Digistat Gateway, prima dell'uso clinico, se i dispositivi scelti non sono quelli menzionati sopra, devono essere effettuate una verifica di compatibilità e una validazione, in accordo alla procedura descritta nel documento Digistat Gateway compatibilty checklist ACDM-585-13656.

3.6 Digistat Web

Le applicazioni Digistat Web sono supportate dai seguenti browser:

- Chrome 140 o successivi;
- Firefox 143 o successivi;
- Edge 140 o successivi.

Il Display Scaling del browser deve essere sempre impostato al 100%.

Non usare diversi browser simultaneamente.

Non usare la modalità di navigazione "In incognito".

Nel caso in cui Digistat Web sia utilizzato per visualizzare le notifiche prodotte dal Clinical Decision Support System, l'organizzazione sanitaria dovrebbe valutare di applicare le seguenti mitigazioni: il browser Web di una workstation Web Digistat deve essere sempre in primo piano. Il browser Web deve essere dedicato solo a Digistat Web e nessun altro utilizzo deve essere consentito. Pertanto, la home page predefinita del browser Web deve essere Digistat Web.

Digistat Web utilizza i cookie per memorizzare informazioni sulla sessione di lavoro corrente. I cookie sono collegati al dominio web delle applicazioni.
Pertanto, se moduli e componenti Digistat Web sono installati su server diversi, è necessario adottare un Load Balancer in modo da utilizzare URL con un dominio web comune consentendo così la coerenza dei cookie.

Inoltre, il Load Balancer deve essere configurato in modo che le chiamate https vengano reindirizzate al server corretto.
Ad esempio: vogliamo installare Vitals Web su un server e Vitals Web API su un altro server. Il Load Balancer deve essere configurato in modo che le chiamate https come https://MYDOMAIN/VitalsWeb vengano instradate al server in cui è installato Vitals Web e le chiamate https come https://MYDOMAIN/VitalsWebAPI vengano instradate all'altro server.

3.7 Ascom Telligence

Digistat Care è compatibile con Ascom Telligence.
Le versioni supportate sono: 6.10, 7.0, 7.1, 7.3, 7.4, 7.5, 7.6.

Tutti i componenti Telligence (server, staff station etc.) devono essere allineati alla stessa versione supportata.

3.8 Avvertenze generali

In caso il Prodotto sia usato per la notifica primaria di allarmi, devono essere installate almeno due postazioni desktop client all'interno dello stesso reparto o, in alternativa, almeno una postazione Digistat Care desktop e una torretta di allarme. Si veda il paragrafo 4.3 per maggiori informazioni.

Per i moduli desktop e mobile, il separatore decimale e, più in generale, le impostazioni locali (ad es. il formato delle date) usati dal Prodotto dipendono dalle impostazioni del sistema operativo della macchina o del dispositivo mobile su cui è installato il Prodotto.
Per i moduli web, il separatore decimale e, più in generale, le impostazioni locali (ad es. il formato delle date) usati dal Prodotto dipendono dalla configurazione del Prodotto.

Per utilizzare correttamente il Prodotto è necessario che il Display Scaling di Microsoft Windows sia impostato al 100%. Impostazioni diverse possono impedire l'esecuzione del prodotto oppure creare malfunzionamenti a livello di rappresentazione grafica. Per impostare il valore Display Scaling consultare la documentazione di Microsoft Windows.

L'organizzazione ospedaliera è tenuta a implementare un meccanismo di sincronizzazione della data ed ora delle workstation su cui gira il Prodotto con una sorgente temporale di riferimento.

È obbligatorio seguire le indicazioni del produttore per l'immagazzinamento, il trasporto, l'installazione, la manutenzione e l'eliminazione dell'hardware di terze parti. Tali operazioni dovranno essere effettuate solo da personale competente e opportunamente addestrato.

I requisiti hardware e software dei dispositivi di terze parti (incluso il modulo Smart Adapter di Project Engineering, i Port Servers di Lantronix, etc.) sono indicati nelle loro istruzioni d'uso, fornite dai rispettivi Produttori. Ascom UMS o i distributori autorizzati possono fornire i contatti dei Produttori dei dispositivi di terze parti.

Il Prodotto è stato verificato e validato durante la fase di installazione o di aggiornamento e il suo collaudo è stato effettuato sull'hardware (PC, server, dispositivi mobili) e sul software (ad es. sistema operativo) insieme ad altri componenti software (ad es. browser, antivirus, ecc.) già presenti. Qualsiasi altro hardware o software installato può compromettere la sicurezza, l'efficacia e i controlli di progettazione del Prodotto.
È obbligatorio consultare Ascom UMS o un Distributore autorizzato prima di utilizzare insieme al Prodotto qualsiasi altro software diverso da quelli validati in fase di installazione o di aggiornamento.
Qualora sia necessario installare qualsiasi altro software (utility o programmi applicativi) sull'hardware su cui gira il Prodotto, l'organizzazione ospedaliera dovrà informare Ascom UMS o un suo Distributore per un'ulteriore validazione. Si suggerisce di applicare una politica di permessi che impedisca agli utenti di eseguire procedure come l'installazione di nuovi software.

3.9 Funzionalità di streaming Audio/Video

In alcune configurazioni il Prodotto implementa funzionalità di streaming audio/video.
Nel caso in cui parti del prodotto fungano da visualizzatore di streaming video, il Prodotto non è la fonte del video e non registra queste informazioni in alcun modo. È responsabilità dell'organizzazione ospedaliera gestire il sistema dal punto di vista della protezione dei dati, compresa l'installazione e la configurazione delle telecamere sorgente.
Nel caso in cui parti del Prodotto trattino audio e immagini relative agli utenti e / o ai pazienti inclusa l'acquisizione, l'elaborazione e la registrazione, è responsabilità dell'organizzazione ospedaliera implementare le procedure necessarie per conformarsi alla normativa locale sulla protezione dei dati, inclusi, a titolo esemplificativo ma non esaustivo, la regolamentazione dell'utilizzo e la definizione della formazione degli utenti.
La funzionalità di streaming video sulle workstation desktop è stata testata con i codec video H264 e H265. Qualsiasi altro codec video presente o installato da applicazioni di terze parti (ad esempio VLC Media Player) deve essere testato prima dell'uso.
Ogni sorgente video supporta un numero massimo di client connessi simultaneamente. È responsabilità dell'organizzazione ospedaliera determinare questo numero massimo e informare gli utenti.
La funzionalità di streaming video su dispositivi mobili supporta solo flussi video RTSP con i seguenti tipi di autenticazione:

- Nessuna autenticazione;
- Autenticazione di base;

- Autenticazione Digest.

La funzionalità di streaming video su dispositivi mobili supporta solo i codec video H263, H264 e H265.

3.10 Firewall e Antivirus

Il contenuto di questo paragrafo è destinato esclusivamente all'utilizzo da parte di tecnici (ad esempio, amministratori di sistema).

Per proteggere il Prodotto da possibili attacchi informatici è necessario che:

- Il Firewall di Windows sia attivo sia sulle workstations che sul server;
- Su workstation e server sia attivo e regolarmente aggiornato un software Antivirus/Antimalware.

È carico dell'organizzazione ospedaliera responsabile assicurarsi che queste due protezioni siano messe in atto. Ascom UMS ha testato il prodotto con l'antivirus WithSecure (F-SECURE in precedenza) facendo uso delle appropriate esclusioni per la cartella "./Server" nella quale è installato Digistat Suite Server. In ogni caso, considerate le politiche e le strategie già in uso nell'organizzazione ospedaliera, la scelta effettiva dell'antivirus è responsabilità dell'organizzazione ospedaliera.

Si consiglia fortemente di mantenere aperte le sole porte TCP ed UDP effettivamente necessarie. Queste possono variare in base alla configurazione del Prodotto. Si raccomanda quindi di rivolgersi all'assistenza tecnica Ascom UMS per tutti i dettagli del caso.

Alcuni antivirus delegano la protezione in tempo reale all'antivirus Microsoft Windows Defender. Controllare sempre, attraverso la sezione "Virus & threat protection" delle impostazioni di Windows, che l'antivirus Windows Defender non sia presente nei server. Se presente, assicurarsi di definire le esclusioni citate sopra per la cartella Digistat Server.

Ascom UMS non può assicurare che Digistat Suite sia compatibile con antivirus o anti-malware diversi da WithSecure (F-SECURE in precedenza).
Sono state riscontrate gravi incompatibilità fra Digistat e altri software antivirus/anti-malware (ad esempio perdite di memoria, tempistiche superiori ai 20 secondi nello scambio di messaggi, ecc.). Assicurarsi di impostare un'esclusione per l'intero folder "./Server" nel quale è installato Digistat Suite Server.
Di seguito una lista di antivirus per i quali sono state riscontrate incompatibilità con Digistat:

- Windows Defender
- Kaspersky
- Trend Micro Apex One

3.10.1 Ulteriori precauzioni raccomandate per la sicurezza informatica

Allo scopo di rafforzare ulteriormente la sicurezza informatica e di proteggere il Prodotto, si raccomanda fortemente di:

- pianificare e implementare lo “Hardening” dell’infrastruttura informatica, inclusa la piattaforma informatica che rappresenta l’ambiente di lavoro del Prodotto,
- implementare un “Intrusion Detection and Prevention System (IDPS) - Sistema di rilevazione e prevenzione delle intrusion informatiche,
- eseguire un test di penetrazione (Penetration Test) e, se in seguito al test è riconosciuta una qualsiasi debolezza, eseguire tutte le azioni necesarie a mitigare il rischio di intrusione informatica,
- mettere fuori uso tutti i dispositivi che non è più possibile aggiornare,
- pianificare ed eseguire una verifica periodica dell’integrità dei file e delle configurazioni,
- implementare una soluzione DMZ (demilitarized zone - zona demilitarizzata) per i server web che devono essere esposti su internet.

3.11 Caratteristiche della rete locale

In questo paragrafo sono elencate le caratteristiche richieste alla la rete locale sulla quale è installato il Prodotto affinché funzioni correttamente.

- il Prodotto utilizza traffico di tipo TCP/IP standard.
- La rete LAN deve essere priva di congestioni e/o saturazioni.
- il Prodotto richiede una LAN di almeno 100 Mbps alle postazioni utente. È auspicabile la presenza di dorsali Ethernet da 1Gbps.
- Non devono essere presenti filtri sul traffico TCP/IP tra workstations, server e dispositivi secondari.
- Se i dispositivi (server, workstation e dispositivi secondari) sono collegati a sottoreti diverse ci deve essere routing tra tali sottoreti.
- Si suggerisce l’adozione di tecniche di ridondanza al fine di assicurare il servizio di rete anche in caso di malfunzionamento.
- Si suggerisce una programmazione condivisa degli interventi di manutenzione programmata in modo che Ascom UMS o il distributore autorizzato possa supportare l’organizzazione ospedaliera nel gestire in modo ottimale i disservizi.

Nel caso si utilizzi una rete WiFi, a causa della possibile intermittenza del collegamento WiFi, si potrebbero avere disconnessioni di rete con conseguente attivazione del “Recovery or Disconnection Mode” che può causare l’indisponibilità del Prodotto nel caso in cui sia usato come sistema primario di notifica degli allarmi. L’organizzazione ospedaliera deve attivarsi per garantire una ottimale copertura e stabilità della rete WiFi e istruire il personale coinvolto sulla gestione delle possibili temporanee disconnessioni.

Ulteriori informazioni sulle caratteristiche richieste della rete locale (inclusa la rete wireless) in cui è installata la Digistat Suite sono disponibili nei Manuali di Installazione e Configurazione della Digistat Suite.

4. Prima di iniziare

4.1 Avvertenze per la manutenzione e l'installazione

Le seguenti avvertenze riguardanti la corretta installazione e la manutenzione del Prodotto devono essere rispettate scrupolosamente.

L'installazione, la manutenzione e le procedure di riparazione devono essere effettuate in accordo alle direttive e linee guida fornite da Ascom/Distributore e solo da tecnici Ascom/Distributore e personale formato e autorizzato da Ascom/Distributore.

Si raccomanda all'organizzazione ospedaliera che fa uso del Prodotto di stipulare un contratto di manutenzione con Ascom UMS o un Distributore autorizzato.

Il Prodotto può essere installato e configurato solo da personale addestrato ed autorizzato. Questo include il personale Ascom UMS o del Distributore autorizzato e ogni altra persona specificamente addestrata e autorizzata da Ascom UMS o dal Distributore. Analogamente, gli interventi di manutenzione e riparazione sul Prodotto possono essere effettuati solo da personale addestrato ed autorizzato e devono rispettare le procedure e linee guida aziendali. Questo include il personale Ascom UMS/Distributore e ogni altra persona specificamente addestrata e autorizzata da Ascom UMS/Distributore.

- Usare solo dispositivi di terze parti raccomandati da Ascom UMS o distributore.
- Solo personale addestrato e autorizzato può installare dispositivi di terze parti.
- L'organizzazione ospedaliera deve assicurare che la manutenzione del Prodotto e di qualsiasi dispositivo di terze parti sia implementata come richiesto al fine di garantirne sicurezza ed efficienza e ridurre il rischio di malfunzionamenti e possibili situazioni di pericolo per il paziente e l'utente.
- La chiave hardware di del Prodotto (dongle USB) se usata deve essere immagazzinata ed utilizzata in condizioni ambientali (temperatura, umidità, campi elettromagnetici, ...) idonee, come specificato dal fabbricante della stessa. Comunque in condizioni sostanzialmente equivalenti a quelle comunemente richieste da dispositivi di elettronica da ufficio.
- L'Organizzazione ospedaliera è responsabile per la selezione delle apparecchiature adatte all'ambiente in cui sono installate ed utilizzate. L'organizzazione ospedaliera deve tra gli altri obblighi considerare la sicurezza elettrica, le emissioni EMC, interferenze dei segnali radio, disinfezione e pulizia. Attenzione dovrà inoltre essere posta ai dispositivi installati nell'area paziente.
- L'organizzazione ospedaliera deve definire procedure di lavoro alternative in caso il Sistema divenga inaffidabile o smetta di funzionare.

4.2 Gestione della Privacy

Precauzioni appropriate devono essere prese al fine di proteggere la privacy di utenti e pazienti, e di assicurare che i dati personali siano elaborati nel rispetto dei diritti dei soggetti coinvolti, delle libertà fondamentali, della dignità personale, con particolare riguardo per la confidenzialità, l'identità personale e il diritto alla protezione dei dati personali

---

Per 'Dati personali' si intende qualsiasi informazione riguardante una persona naturale identificata o identificabile ('soggetto dei dati'); una persona naturale identificabile è un individuo che possa essere identificato, direttamente o indirettamente, in particolare in riferimento a un identificatore quale un nome, un numero identificativo, dati relativi a luoghi, un identificativo telematico o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di quella persona naturale.

Attenzione particolare deve essere dedicata ai dati definiti nel "EU general data protection regulation 2016/679 (GDPR)" come "Categorie Speciali di dati personali".

Categorie speciali di dati personali:
(...) Dati personali che rivelino origini razziali o etniche, opinion politiche, convinzioni religiose o filosofiche, appartenenza a sindacati, e (...) dati genetici, dati biometrici che abbiano il solo scopo di identificare una persona naturale, data riguardanti lo stato di salute o riguardanti la vita sessuale o l'orientamento sessuale di una persona naturale.

L'organizzazione ospedaliera deve assicurare che l'utilizzo del Prodotto è in linea con i requisiti definiti dalla legislatura applicabile sulla privacy e sulla protezione dei dati personali, in particolare rispetto alla gestione dell'informazione menzionata sopra.

Il Prodotto gestisce e mostra dati personali.

Il prodotto può essere configurato in modo da nascondere automaticamente nelle schermate dell'applicazione, quando nessun utente è loggato, il sottoinsieme dei dati personali che possono essere utilizzati per identificare una persona fisica.
I campi nascosti sono:

- Nome e cognome
- Data di nascita
- Sesso
- Codice paziente
- Data di ammissione
- Data di dimissione
- Peso del paziente
- Altezza del paziente

Il set dei campi nascosti può essere personalizzato in fase di configurazione del Prodotto.
Per fare ciò, sull'applicazione di configurazione del Prodotto, si imposti la "System Option" denominata "Privacy Mode" a "true" (si veda il manuale di configurazione e installazione del prodotto) per la procedura dettagliata). Il valore impostato di default è "true".

Se l'opzione "Privacy Mode" è impostata su "true", sono possibili i seguenti casi:

- se non c'è un utente loggato, non è visualizzata alcuna informazione relativa al paziente.
- se c'è un utente loggato, e l'utente non ha un permesso specifico, non è visualizzata alcuna informazione relativa al paziente.
- se c'è un utente loggato, e l'utente ha il permesso specifico, sono visualizzate le informazioni relative al paziente.

L'opzione può essere applicata a una singola postazione di lavoro (cioè, diverse postazioni possono essere configurate in modo differente).

Leggere attentamente le precauzioni esposte nel presente paragrafo ed osservarle scrupolosamente.

- I PC in uso non devono rimanere incustoditi e accessibili durante le sessioni di lavoro con il Prodotto. Si raccomanda di eseguire il log out dal Prodotto quando ci si allontana dalla postazione di lavoro.
- I dati sensibili immessi nel Prodotto, quali password o dati personali degli utenti e dei pazienti devono essere protetti da qualsiasi tentativo di accesso non autorizzato attraverso software adeguati (antivirus e firewall). L'implementazione di tali software è di competenza dell'organizzazione ospedaliera. Tali software devono essere regolarmente aggiornati.
- L'utente è avvisato che l'uso frequente della funzione "blocca utente" è potenzialmente pericoloso. Il "Log out" automatico protegge il Prodotto dagli accessi non autorizzati.
- Dati personali possono essere presenti in alcune delle stampe generate dal Prodotto. L'organizzazione ospedaliera deve gestire questi documenti in accordo alla legislatura corrente sulla privacy e sulla protezione dei dati personali.
- Le postazioni di lavoro client (sia desktop sia mobili) non salvano su disco i dati-paziente. I dati del paziente sono salvati solo su database e il tipo di salvataggio su database dipende dalle scelte e dalle procedure adottate dall'organizzazione ospedaliera che usa il Prodotto (esempi: macchine fisiche, SAN - Storage Area Network -, ambienti virtuali). I dati del paziente dovranno essere gestiti secondo le normative vigenti sulla privacy e sulla protezione dei dati personali.
- L'organizzazione ospedaliera deve provvedere ad un addestramento del personale riguardo alle nozioni fondamentali riguardanti la privacy: ad esempio i principi base, le regole da seguire, i regolamenti in vigore, le responsabilità e le sanzioni relativamente all'ambiente di lavoro specifico di ognuno. Ascom UMS o il Distributore possono provvedere ad un addestramento dettagliato riguardo al miglior uso del Prodotto relativamente alla privacy (ad esempio: anonimizzazione dei database, modalità "private", permessi degli utenti etc.).
- L'organizzazione ospedaliera dovrà produrre e conservare la seguente documentazione:
  1. la lista aggiornata degli amministratori di sistema e del personale addetto alla manutenzione del Prodotto;
  2. i moduli di assegnazione dei ruoli firmati e le certificazioni di presenza ai corsi di addestramento;
  3. un registro delle credenziali, dei permessi e delle prerogative degli utenti;
  4. una lista aggiornata degli Utenti del prodotto.

- L’organizzazione ospedaliera dovrà implementare, verificare e certificare un meccanismo di disattivazione automatica degli utenti non più attivi per un determinato periodo di tempo.
- L’organizzazione ospedaliera dovrà codificare, implementare e documentare una procedura per la verifica periodica della corrispondenza al ruolo di amministratore di sistema e di tecnico addetto alla manutenzione del Prodotto.
- L’organizzazione ospedaliera dovrà eseguire verifiche formali e controlli sul corretto comportamento degli utenti del prodotto.

I database contenenti dati personali dei pazienti o informazioni sensibili non possono lasciare l’organizzazione ospedaliera senza che siano stati prima offuscati o criptati

I dati del paziente non sono salvati su file proprietari. I dati del paziente sono salvati solo su database.

In alcune circostanze dati personali sono trasmessi in formato non criptato e utilizzando una connessione non intrinsecamente sicura. Un esempio di questa situazione sono le comunicazioni HL7. È responsabilità dell'organizzazione ospedaliera prevedere, all'interno della rete ospedaliera, adeguati meccanismi di sicurezza in modo da assicurare la conformità con le leggi e i regolamenti concernenti la privacy.

4.2.1 Caratteristiche e uso delle credenziali di accesso

Questo paragrafo fornisce indicazioni sulle caratteristiche che devono avere le credenziali di accesso al Prodotto (nome utente e password) e sulle loro modalità di utilizzo e mantenimento.

- Ogni utente deve prendere tutte le precauzioni possibili per mantenere segreti il proprio nome utente e la propria password.
- Nome utente e password sono private e personali. Non comunicare mai a nessuno il proprio nome utente e la propria password.
- Ogni incaricato può avere una o più credenziali per l’autentificazione (nome utente e password). Gli stessi nome utente e password non devono essere utilizzati da più incaricati.
- I profili di autorizzazione devono essere controllati e rinnovati almeno una volta all’anno.
- È possibile raggruppare diversi profili di autorizzazione in base all’omogeneità dei compiti degli utenti.
- Ogni account utente deve essere collegato con una persona specifica. L’uso di utenti generici (come, ad esempio, “ADMIN” o “INFERMIERE”) deve essere evitato. In altre parole, per ragioni di tracciabilità è necessario che ogni account sia utilizzato da un solo utente.
- Ogni utente è caratterizzato da un profilo che gli permette di utilizzare soltanto le funzionalità del Prodotto che sono pertinenti ai suoi compiti. L’amministratore di

sistema deve assegnare il profilo adeguato contestualmente alla creazione dell'account utente. Tale profilo deve essere rivisto almeno una volta all'anno. Tale revisione può avvenire anche per classi di utenti. Le procedure relative alla definizione del profilo dell'utente sono descritte nel manuale di configurazione del Prodotto.

- La password deve essere composta da almeno otto caratteri.
- La password non deve contenere riferimenti agevolmente riconducibili all'incaricato (ad esempio nome, cognome, data di nascita etc.).
- La password è assegnata dall'amministratore di sistema e deve essere modificata dall'utente al primo utilizzo del Prodotto, se ciò è espressamente stabilito da configurazione (si veda il documento *USR ITA Control Bar* per la procedura di modifica della parola chiave).
- Successivamente, la password deve essere modificata almeno ogni tre mesi.
- Se le credenziali di accesso (nome utente e password) rimangono inutilizzate per più di sei mesi devono essere disattivate. Fanno eccezione credenziali specifiche da utilizzare per scopi di manutenzione tecnica. Si veda il manuale di configurazione del Prodotto per la procedura di configurazione di questa caratteristica.
- Le credenziali di accesso sono disattivate anche in caso di perdita da parte dell'utente della qualifica corrispondente a tali credenziali (è il caso, ad esempio, in cui un utente si trasferisca ad un'altra struttura). L'amministratore di sistema può abilitare/disabilitare manualmente un utente. La procedura è descritta nel manuale di configurazione del Prodotto.

Le seguenti informazioni sono di pertinenza dei tecnici amministratori di sistema:

La parola chiave deve rispettare una regular expression definita nella configurazione del Prodotto (Il default è ^.....* cioè 8 caratteri).
La password è assegnata dall'amministratore di sistema nel momento in cui è creato un nuovo account per un utente. L'amministratore può obbligare l'utente a modificare tale password e sostituirla con una personale la prima volta che accede al Prodotto. La password scade dopo un periodo di tempo configurabile, l'utente è tenuto a cambiare la password allo scadere di tale periodo. È possibile fare in modo che la password di un utente non scada.

Si veda il manuale di configurazione del Prodotto per informazioni dettagliate sulla definizione degli account utente e sulla configurazione delle password.

4.2.2 Amministratori di sistema

Nello svolgere le normali attività di installazione, aggiornamento ed assistenza tecnica del Prodotto il personale Ascom UMS o dei Distributori autorizzati potrà aver accesso e trattare dati personali e sensibili memorizzati nel database e agire da Amministratori di Sistema per il Prodotto.
Ascom UMS adotta procedure ed istruzioni di lavoro che sono conformi alle prescrizioni della vigente normativa sulla privacy ("General Data Protection Regulation - EU 2016/679").

Si consiglia all'organizzazione ospedaliera di prendere in considerazione, fra le altre, le seguenti misure:

- definire gli accessi in modo nominativo;
- attivi il log degli accessi a livello di sistema operativo sia sul server che sui client;
- attivi il log degli accessi al database server Microsoft SQL Server (Audit Level);
- configuri e gestisca entrambi questi log in modo da mantenere traccia degli accessi per un periodo di almeno un anno.

4.2.3 Log di sistema

Il Prodotto registra i log di sistema sul database. Tali log sono mantenuti per un periodo di tempo che è configurabile. I log sono mantenuti per periodi di tempo differenti a seconda della loro natura. Di default le tempistiche sono le seguenti:

- i log informativi sono mantenuti per 10 giorni;
- i log corrispondenti a warning sono mantenuti per 20 giorni;
- i log corrispondenti a errori sono mantenuti per 30 giorni.

Queste tempistiche sono configurabili. Si veda il manuale di configurazione del Prodotto per la procedura di definizione delle tempistiche di mantenimento dei log.

4.2.4 Log Forensi

Un sottoinsime dei suddetti log di sistema, definiti come "clinicamente rilevanti" o "clinicamente utili" in base alle politiche adottate da ogni specifica organizzazione ospedaliera che utilizzi il Prodotto, possono essere inviati a sistemi esterni (o SQL o Syslog) per essere qui immagazzinati in base ai regolamenti e alle necessità dell'organizzazione ospedaliera stessa.

4.3 Dispositivi compatibili

4.3.1 Dispositivi di tipo DAS

Dispositivi che consentono l'implementazione di un Sistema distribuito di allarme affidabile ("reliable distributed alarm system").
I dati acquisiti da questo tipo di dispositivi sono visualizzati su Digistat Care.
I dati acquisiti da questo dispositivo possono essere inviati in uscita come HL7. Gli output HL7 non sono però affidabili (reliable)

- *Ventilatore Hamilton S1 e C6 e altri modelli che supportano lo stesso protocollo*
- *Pompe di infusione Arcomed Syramed µSP6000 e Volumed µVP7000 connesse al rack Arcomed UniQueConcept (e altri dispositivi che supportano lo stesso protocollo).*
- *Dispositivi medici collegati al Targeted Alarm Service (TAS) Dräger.*

Per usare i dispositivi supportati in un sistema distribuito di allarme è necessario configurare in modo appropriato i settaggi di comunicazione dei dispositivi stessi come indicato nella documentazione tecnica.

Dispositivi Hamilton
Il ventilatore Hamilton supporta l'opzione "Terapia Intensiva silenziosa" ("Silent ICU Option"). Ciò significa che può essere usato insieme a Digistat Care per operare in modalità silenziosa. Per usare il ventilatore Hamilton in un sistema distribuito di allarmi come ventilatore silenzioso (ad esempio, in una TI silenziosa), è possibile farlo funzionare nello stato AUDIO OFF.
In primo luogo, il ventilatore deve essere correttamente configurato. Si veda la documentazione tecnica del dispositivo per le istruzioni di configurazione e le istruzioni dettagliate su come farlo funzionare in modalità silenziosa (stato AUDIO OFF).

Si faccia riferimento alla documentazione tecnica del ventilatore Hamilton per istruzioni più dettagliate.

Il ritardo massimo misurato in ambiente di test fra la visualizzazione di una notifica sul ventilatore e la visualizzazione della stessa sul Prodotto è di 600 ms.
Il ritardo Massimo misurato in ambiente di test fra la visualizzazione di una notifica sul ventilatore e la visualizzazione della stessa sul Prodotto in versione Mobile è di 1000 ms.

Il ritardo massimo misurato in ambiente di test fra la connessione del ventilatore Hamilton e la visualizzazione dei dati sul Prodotto è 22900 ms.
Il ritardo massimo misurato in ambiente di test fra la connessione del ventilatore Hamilton e la visualizzazione dei dati sul Prodotto versione mobile è 20233 ms.

Possono essere necessari fino a due secondi di tempo fra la generazione di un allarme e l'invio dello stesso sul ventilatore Hamilton.
Il ventilatore poi attende un messaggio di conferma da Digistat Care. Se tale conferma non è ricevuta entro altri due secondi, c'è un timeout.
Perciò, il ritardo massimo oltre il quale la notifica di allarme è fornita è di 4 secondi.
In caso di timeout:

- Viene inviato un allarme di connessione. L'allarme può essere rimosso dall'utente oppure è rimosso se è stabilita una nuova connessione con conferma di ricezione.
- È rimosso qualsiasi silenzio attivo.
- L'invio dati da parte del ventilatore e la conferma di ricezione si ferma finché non è stabilita una nuova connessione.

Se i ventilatori Hamilton sono configurati come parte di un Distributed Alarm System, lo stato di AUDIO OFF è disabilitato automaticamente se si verifica una delle seguenti condizioni:

- Il driver Hamilton risulta non disponibile;
- Il Sistema DAS risulta non affidabile.

Dispositivi Arcomed

Il rack / La pompa Arcomed supporta l'opzione "Terapia Intensiva silenziosa" ("Silent ICU Option"). Ciò significa che può essere usato insieme a Digistat Care per operare in modalità silenziosa.

Per usare il rack / la pompa Arcomed in un sistema distribuito di allarmi come rack / pompa silenzioso (ad esempio, in una TI silenziosa), è possibile farlo funzionare nello stato AUDIO OFF.

In primo luogo, il rack / la pompa Arcomed deve essere correttamente configurato. Si veda la documentazione tecnica del dispositivo per le istruzioni di configurazione e le istruzioni dettagliate su come farlo funzionare in modalità silenziosa (stato AUDIO OFF).

Si faccia riferimento alla documentazione tecnica del rack/pompa Arcomed per istruzioni più dettagliate.

Il ritardo massimo misurato in ambiente di test fra la visualizzazione di una notifica sulla pompa/rack Arcomed e la visualizzazione della stessa sul Prodotto è di 3927 ms.
Il ritardo Massimo misurato in ambiente di test fra la visualizzazione di una notifica sulla pompa/rack Arcomed e la visualizzazione della stessa sul Prodotto in versione Mobile è di 4350 ms.

Possono essere necessari fino a 10 secondi di tempo fra la generazione di un allarme e l'invio dello stesso sulla pompa / rack Arcomed.
La pompa / rack poi attende un messaggio di conferma da Digistat Care. Se tale conferma non è ricevuta entro venti secondi, c'è un timeout.
Perciò, il ritardo massimo oltre il quale la notifica di allarme è fornita è di 20 secondi.
In caso di timeout:

- Viene inviato un allarme di connessione. L'allarme può essere rimosso dall'utente oppure è rimosso se è stabilita una nuova connessione con conferma di ricezione.
- È rimosso qualsiasi stato di AUDIO OFF attivo.
- Se è ristabilita una connessione con conferma di ricezione e se Digistat Care è in stato "Reliable", la modalità silenziosa (stato AUDIO OFF) è ripristinato automaticamente dalle pompe di infusione.
- Digistat Care cerca di ripristinare la comunicazione.

Il ritardo massimo misurato in ambiente di test fra la connessione della pompa/rack Arcomed e la visualizzazione dei dati sul Prodotto è 63 s.
Il ritardo massimo misurato in ambiente di test fra la connessione della pompa/rack Arcomed e la visualizzazione dei dati sul Prodotto versione mobile è 63 s.

Le pompe di infusione Arcomed richiedono una rete separate per funzionare come parte di un "Distributed Alarm System". "Rete separata" significa: diversa rete fisica, VLAN o subnets con IP separati. Ciò è necessario per prevenire possibili conflitti con specifiche politiche di sicurezza di rete, come indicato dal fabbricante della pompa/rack.

Se le pompe Arcomed sono configurate come parte di un Distributed Alarm System, lo stato di AUDIO OFF è disabilitato automaticamente se si verifica una delle seguenti condizioni:

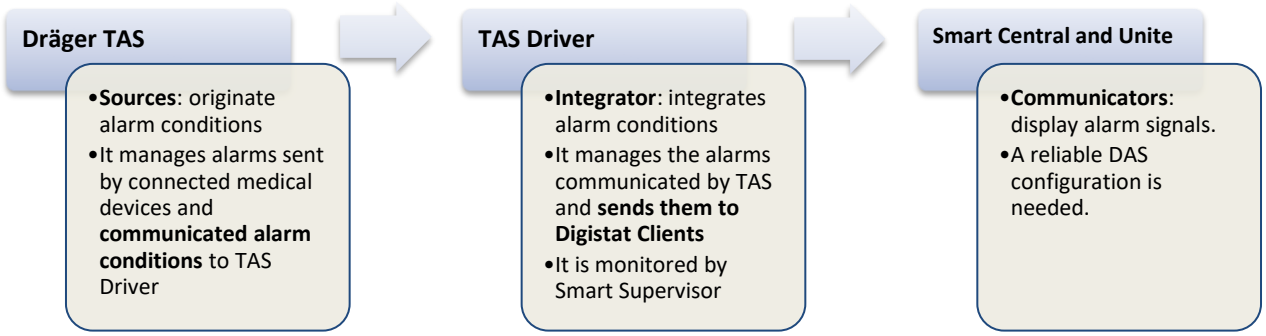
- Il driver Arcomed risulta non disponibile;
- Il Sistema DAS risulta non affidabile.

Il driver Arcomed è un driver multiletto, quindi un singolo rack può essere in stato non affidabile mentre gli altri lavorano in stato affidabile.

Dispositivi medici collegati al Targeted Alarm Service (TAS) Dräger.

In un "Distributed Alarm System" con TAS Dräger, devono essere presenti almeno due Dispositivi Medici (AlertProvider) con il più breve tempo di autocontrollo (Selfcheck time). Consultare le istruzioni per l'uso del server TAS Dräger per ulteriori informazioni.

Il **driver Targeted Alarm Service** (TAS) funziona come gateway di allarme e **"integratore"** (secondo lo standard IEC 60601-1-8:2020) delle **condizioni di allarme** originate da **dispositivi medici** connessi alla rete privata Dräger. I dispositivi medici facenti parte della rete privata Dräger comunicano con il **Dräger Targeted Alarm Service gateway** (TAS gateway) secondo il protocollo di comunicazione standard SDC (IEEE 11073). Il TAS Dräger inoltra la notifica di condizioni di allarme al Driver TAS che le invia ai **comunicatori Digistat**, come Smart Central e Unite, dove alla fine vengono visualizzate le segnalazioni di allarme.



Il TAS comunica al TAS Driver, attraverso le API TAS versione 1.1, le condizioni di allarme dei dispositivi collegati alla rete TAS (fino a 100 dispositivi per TAS). Il driver TAS supporta una connessione criptata e l'autenticazione secondo i requisiti di sicurezza TLS 1.2. La correttezza dei messaggi è garantita dal protocollo TCP/IP.

Il driver TAS è un driver di tipo DAS e supporta lo stato **Global AUDIO OFF** attivo sui dispositivi medici. Insieme al Dräger Targeted Alert Service, può essere configurato per implementare **un sistema di allarme distribuito** (DAS), che richiede una configurazione affidabile (reliable) con **Smart Supervisor** attivo ("System Option" *SmartCentralMode* impostata su **Reliability** o **Monitoring and Reliability**) e **doppia Smart Central**.

Il TAS può inviare avvisi in più lingue contemporaneamente. Di default il driver usa la lingua impostata per il Data Acquisition Node (“System Option” *Language* con applicazione *DASNODE*). È possibile sovrascrivere la lingua e impostare una o più lingue sul driver TAS. Nel caso in cui la lingua dell'avviso ricevuto dai dispositivi medici sia diversa da quella configurata nelle impostazioni del TAS, la lingua dell'avviso sarà riportata insieme al testo dell'allarme ricevuto dal dispositivo TAS e a un avviso che indica l'impossibilità di fornire una traduzione diversa.

⚠ Durante la configurazione, il parametro personalizzato *BedNameFormat* deve essere impostato nella pagina Edit Device Driver > Custom Parameters > Custom tab (Configurator Web > Connect > Drivers > Device driver management, quindi selezionare l'istanza del driver TAS) dell'istanza del driver TAS per gestire la mappatura dei letti.

⚠ A seconda della configurazione dei dispositivi collegati al TAS, è possibile utilizzare lingue miste per i testi degli allarmi.

Se il Prodotto è utilizzato come Sistema primario di notifica di allarmi, qualunque dispositivo fisico ad esso collegato tramite il dispositivo TAS di Dräger che supporta l'abilitazione della modalità GLOBAL AUDIO OFF (così come definita da IEC 60601-1-8), deve disabilitare il GLOBAL AUDIO OFF nel caso in cui:

- ci sia un malfunzionamento del Sistema Distribuito di Allarme oppure
- ci sia una disconnessione del dispositivo fisico (ad esempio dalla rete ospedaliera, dal TAS, dal sistema distribuito di allarmi etc.).

Il tecnico incaricato della configurazione del Digistat TAS Driver deve verificare che il certificato ricevuto da Dräger corrisponda a quello utilizzato dal TAS Server utilizzando almeno due mezzi diversi (ad esempio, per posta elettronica e a voce).

Le misure sui ritardi sono state effettuate su un ventilatore Dräger Babylog VN800 collegato a una rete privata Dräger.
Il ritardo Massimo misurato in ambiente di test tra la visualizzazione della notifica sul Dräger Babylog VN800 e la visualizzazione della notifica sul Prodotto è di 500 ms. Il ritardo massimo misurato in ambiente di test tra la visualizzazione della notifica sul Dräger Babylog VN800 e la visualizzazione della notifica sul Prodotto (versione Mobile) è di 900 ms.

Vitalthings Guardian Gateway

Il driver Vitalthings Guardian Gateway è compatibile con Vitalthings Guardian Gateway versione 1.0.2, protocollo versione 1.0.
I monitor paziente Vitalthings Guardian M10, integrati tramite Vitalthings Guardian Gateway, possono essere configurati come parte di un CDAS (Distributed Alarm System with Confirmed delivery- "*sistema di allarme distribuito con consegna confermata*").
La versione del firmware supportata del monitor paziente Vitalthings Guardian M10 è la 2.0.2.

Nel caso in cui i monitor paziente Vitalthings Guardian M10, integrati tramite Vitalthings Guardian Gateway, siano configurati come parte di un SISTEMA DI ALLARME DISTRIBUITO CON CONSEGNA CONFERMATA, il monitor paziente Guardian M10 ha il ruolo di SORGENTE di allarme e Digistat ha il ruolo di INTEGRATORE di allarmi e COMUNICATORE di allarmi.

Per istruzioni dettagliate, fare riferimento alla documentazione di Vitalthings Guardian Gateway e Vitalthings Guardian M10.

Quando il driver Vitalthings riceve una notifica di inaffidabilità dal "Supervisor" (problema globale o problema del letto singolo), il driver non inoltra alcuna richiesta di CONFERMA al monitor paziente.

	Il monitor paziente Vitalthings Guardian M10 può scartare una richiesta di CONFERMA se non corrisponde allo stato di allarme corrente del monitor.

	I monitor paziente VitalThings non implementano GLOBAL AUDIO OFF, ma solo una richiesta di RICONOSCIMENTO temporizzato remoto per lo stato di inattivazione del SEGNALE DI ALLARME da parte dell'INTEGRATORE di allarmi. Quando una richiesta di RICONOSCIMENTO temporizzato viene accettata dal monitor paziente Guardian M10, l'audio viene temporaneamente messo in pausa per un numero di minuti configurabile sul monitor paziente (ad es. 2 minuti)

	Il ritardo massimo misurato in un ambiente di test tra la connessione del dispositivo Vitalthings Guardian M10 e la visualizzazione dei dati su Digistat Care è di 130 ms. Il ritardo massimo misurato in un ambiente di test tra la connessione del dispositivo Vitalthings Guardian M10 e la visualizzazione dei dati su Digistat Care (versione Mobile) è di 290 ms.

	Il ritardo massimo misurato in un ambiente di test tra la visualizzazione delle notifiche sul dispositivo Vitalthings Guardian M10 e la visualizzazione delle notifiche su Digistat Care è inferiore a 4 ms. Il ritardo massimo misurato in un ambiente di test tra la visualizzazione delle notifiche sul dispositivo Vitalthings Guardian M10 e la visualizzazione delle notifiche su Digistat Care (versione mobile) è di 160 ms.

	Il ritardo massimo misurato in un ambiente di test tra la connessione al wireless sul dispositivo Vitalthings Guardian M10 e la visualizzazione delle notifiche su Digistat Care è di 32000 ms. Il ritardo massimo misurato in un ambiente di test tra la connessione al wireless sul dispositivo Vitalthings Guardian M10 e la visualizzazione delle notifiche su Digistat Care (versione mobile) è di 32000 ms.

4.3.2 Dispositivi di tipo DIS

Dispositivi che non consentono l'implementazione di un sistema distribuito di allarme affidabile ("reliable distributed alarm system"). Questa comunicazione non è affidabile (reliable), perciò non può essere utilizzata per implementare un sistema distribuito di allarme affidabile. Può invece essere utilizzato per implementare un Sistema distribuito di informazione ("Distributed Information System").

Si prega di contattare Ascom UMS /Distributore per la lista aggiornata dei dispositivi.

Per ragioni che non sono sotto il controllo del software (come, ad esempio, il modo in cui gli effettivi dispositivi fisici sono installati o cablati) potrebbero esserci dei ritardi fra il momento in cui la notifica è generata e il momento in cui è visualizzata.

L'aggiornamento dei dati visualizzati sullo schermo dovuto alla connessione di un nuovo dispositivo, a spegnimento, a disconnessione e modifica di stato, dipende dal tempo necessario al dispositivo stesso per comunicare le modifiche. Questa arco temporale dipende da vari fattori, fra i quali il tipo di dispositivo e il tipo di connessione. Per alcuni dispositivi esistono condizioni nelle quali il ritardo nella comunicazione delle modifiche può essere significativo. Non è possibile indicare i ritardi per tutti i dispositivi possibili perché tali ritardi variano a seconda delle configurazioni e delle condizioni operative.

I drivers usati per leggere i dati dai dispositivi medici collegati hanno un ciclo di lettura inferiore ai tre secondi (cioè: tutti i dati dai dispositivi sono letti ogni tre secondi al massimo). Esistono dispositivi che comunicano informazioni meno di frequente (ad esempio ad intervalli di 5-10 secondi). Si faccia riferimento alla documentazione specifica del driver per dettagli riguardo al ciclo di lettura.
In un ambiente di test installato e configurato come indicato nel manuale di installazione e configurazione del Prodotto, appena un driver riconosce un allarme, è necessario un secondo al massimo per trasferirlo al Prodotto.

4.3.3 Avvertenze

Il Prodotto riceve dati da diverse fonti: dispositivi medici, Sistema Informatico Ospedaliero, dall'utente, inseriti manualmente.
Inoltre il Prodotto calcola informazioni derivate (ad esempio i Severity Scores).
La precisione, l'accuratezza e la gamma di valori di tali dati dipendono da fonti esterne, da ciò che l'utente inserisce, dall'hardware usato e dall'architettura software.

A seconda delle caratteristiche dei dispositivi medici collegati, il Prodotto può essere usato per la notifica di allarmi primaria (DAS/CDAS) o secondaria (DIS). La presenza di un singolo dispositivo DIS fa sì che l'applicazione mostri un segnale di attenzione che informa che alcuni dei dispositivi collegati non supportano la notifica di allarmi primaria.

Il Prodotto non è stato progettato per verificare il corretto funzionamento dei dispositivi.

La disconnessione di un dispositivo durante il suo funzionamento causa l'interruzione dell'acquisizione dei dati da parte del Prodotto. I dati del dispositivo che sono persi nel periodo di disconnessione non sono recuperati dal Prodotto dopo che il dispositivo è di nuovo connesso.

Non disabilitare mai i sistemi di allarme sui dispositivi medici al di fuori dei casi indicati dalla documentazione fornita dal produttore del dispositivo stesso e dalle procedure in uso nell'organizzazione ospedaliera.

L'organizzazione ospedaliera deve garantire (ad es. tramite appropriate checklist) che la ricezione corretta degli allarmi sia gestita nel Prodotto sia che la notifica Sonora sia disabilitata, sia che sia abilitata per un paziente specifico sul dispositivo mobile.

Nel caso ci sia una pompa di infusione collegata al Prodotto, non modificare il numero seriale della pompa.

Mai disabilitare l'audio delle postazioni sulle quali è installato dal Prodotto.

Se il driver generico Alaris® è in uso, dopo aver scollegato una pompa di infusione, è necessario attendere almeno dieci secondi prima di collegarne un'altra.

Livelli di pressione acustica (volume sonoro) inferiori a quelli ambientali possono impedire la corretta percezione degli allarmi da parte dell'utente.

A seconda di quanto deciso dall' Organizzazione ospedaliera, il Prodotto potrebbe essere configurato per filtrare e/o rimappare gli allarmi generate dai dispositivi medici collegati.
Gli utenti devono essere consapevoli che, a seconda della configurazione, gli allarmi potrebbero essere presentati con una diversa priorità o un diverso messaggio oppure potrebbero non essere annunciati.
L' Organizzazione ospedaliera ha la responsabilità di fornire informazioni e addestramento agli utenti a proposito della configurazione del filtraggio degli allarmi.
Gli utenti dovranno essere informati di ogni successivo cambiamento alla configurazione del filtraggio degli allarmi.

L'Operatore è in grado di leggere le notifiche del Prodotto fino a una distanza di 1m (3,28 piedi). Entro una distanza massima di 4m (13,12 ft) per l'Operatore è possibile vedere che c'è una notifica. Questo è vero se:

- L'Operatore ha una capacità visiva pari a 0 sulla scala logMAR o acuità visiva pari 6-6 (20/20). (Corretta, se necessario),
- Il punto di vista è localizzato alla postazione dell'Operatore o in un punto compreso alla base di un cono sotteso da un angolo di
- 30° rispetto all'asse orizzontale o al centro del piano di visualizzazione del dispositivo di indicazione visiva
- L'illuminazione dell'ambiente è compresa fra 100 lx e 1 500 lx.

La struttura ospedaliera, in accordo alla propria politica di gestione del rischio e in base al tipo di ambiente nel quale Digistat Care è operativo (ad esempio: dimensioni del monitor, impostazioni dei colori, posizione del PC all'interno della corsia ecc.), può definire la distanza massima dell'operatore affinché sia rilevata la presenza di allarmi.

Periodicamente (ad esempio all'inizio di ogni turno) si verifichi sulla postazione centrale che per ogni letto i dati provenienti dai dispositivi medici collegati siano visualizzati correttamente.

Si usi la procedura di controllo del suono per verificare se l'audio sulla postazione di lavoro/dispositivo mobile sta funzionando correttamente (si vedano i documenti *USR ITA Smart Central* e *USR ITA Mobile Launcher* per la procedura da eseguire su desktop o su mobile). Se i moduli Smart Central / Smart Central Mobile non sono installati, allora tale procedura non è rilevante.

Il Prodotto acquisisce l'informazione generata dai dispositivi medici primari e la visualizza. Perciò, Il Prodotto riporta sempre ciò che i dispositivi medici primari comunicano. L'assegnazione delle priorità agli allarmi è decisa in accordo a quanto stabilito sui dispositivi medici primari. Sul Prodotto è possibile decidere l'ordine dei dispositivi medici, su ogni letto, in accordo alle preferenze del cliente: per tipo di dispositivo, fabbricante, modello. Tale ordinamento viene deciso in fase di implementazione del prodotto in accordo alle richieste e alle preferenze del cliente. Il colore di ogni area-letto è sempre il colore dell'allarme con priorità più alta fra tutti quelli in corso su quel letto.

4.4 Distribuzione di allarmi sicura su guasto singolo (“Single Fault Safe”)

A seconda delle caratteristiche dei dispositivi medici collegati, il prodotto può essere “single fault safe” rispetto alla distribuzione degli allarmi, se installato e configurato di conseguenza. Questo significa che ogni singola parte del Sistema che è coinvolta nella distribuzione degli allarmi è costantemente monitorata, incluso il “Controller” stesso (cioè l’agente che realizza il monitoraggio sulle altre parti del Sistema) e, se si verifica un guasto su una parte qualsiasi del Sistema, viene inviata una notifica agli utenti. In caso di guasto, Digistat Care smette di funzionare finché la causa del guasto è identificata e rimossa.
Per quanto riguarda le postazioni di lavoro portatili (i dispositivi Myco), nelle stesse condizioni descritte sopra viene fornita una notifica a tutti i dispositivi collegati. Questa notifica ha lo stesso livello di severità di un allarme clinico e non può essere rimossa finché non ne siano state rimosse le cause.

Per assicurare la sicurezza su guasto singolo (“single fault safety”), almeno due postazioni di lavoro desktop Digistat Care devono essere installate nello stesso reparto oppure, in alternativa, almeno una postazione Digistat Care e una torretta di allarme luminoso.

Ogni postazione di lavoro o torretta può così monitorare il corretto funzionamento degli altri componenti. Le postazioni di lavoro desktop e la torretta luminosa hanno anche la funzione di monitorare il “Controller”. Si veda il manuale di configurazione di Digistat Care per una descrizione dettagliata dell’architettura del Prodotto.

L’organizzazione ospedaliera deve implementare adeguate procedure interne per assicurare la presenza di almeno un membro dello staff clinico vicino a ciascuna postazione Desktop e alla torretta di allarme, se presente, per essere prontamente consapevole di qualsiasi allarme si verifichi.

L’organizzazione ospedaliera che fa uso di Digistat Care dovrà implementare procedure adeguate a riportare il Prodotto alla sua piena funzionalità nel minor tempo possibile.

Inoltre, l’organizzazione ospedaliera deve definire procedure di lavoro alternative in caso il Sistema divenga inaffidabile o smetta di funzionare.

4.4.1 Torretta di allarme luminosa

Digistat Care è progettato per comunicare tramite un protocollo standard con una torretta di allarme luminoso acquistabile da terzi. Quando Digistat Care è installato e configurato per la distribuzione affidabile di allarmi, la torretta fornisce notifiche informative visive e sonore, informando gli utenti in modo ridondante se il sistema funziona correttamente o no.
La torretta luminosa può essere usata come alternativa alla seconda postazione Digistat Care, che altrimenti è obbligatoria per la distribuzione affidabile degli allarmi.
La presenza della torretta luminosa dipende da una system option. Se la torretta luminosa è presente, allora il sistema può essere validato come affidabile anche con una sola postazione Digistat Care. Si veda il manuale di configurazione del Prodotto per maggiori informazioni.
Sulla torretta:

- Se il Sistema funziona correttamente la luce verde è accesa. Nessun suono è prodotto;
- Se c'è un allarme tecnico (un errore di Sistema, si vedano i paragrafi 4.5 e 4.5.3) si accendono la luce rossa e un allarme sonoro;
- la luce rossa e l'allarme sonoro si accendono anche quando la comunicazione fra la torretta e lo Smart Supervisor (il "controllore" menzionato sopra) si interrompe; allo stesso tempo lo Smart Supervisor produce un allarme tecnico quando la comunicazione con la torretta si interrompe.

Digistat Care è stato verificato con la "Network Monitor Signal Tower" di Patlite, ma altri modelli potrebbero essere compatibili con Digistat Care. Per maggiori informazioni si contatti l'assistenza tecnica di Ascom UMS/Distributore.

La "Network Monitor Signal Tower" di Patlite è una torre di segnalazione su tre livelli con un dispositivo sonoro. Può notificare immediatamente, attraverso una connessione di rete, quando si verifica un evento di rete.

Fig 1

4.5 Inaffidabilità del sistema

In caso il sistema divenga inaffidabile, la notifica di uno specifico "Errore di Sistema" è fornita sia sulle postazioni desktop (Fig 2), sia sui dispositivi portatili, sia sulla torretta opzionale (luce rossa e allarme sonoro accesi).

In caso di "Errore di Sistema" in tutti i letti coinvolti non sono visualizzati dati-paziente finché il Sistema non torni di nuovo affidabile.

Le possibili cause di inaffidabilità sono elencate nel paragrafo 4.5.3.

4.5.1 Desktop

Sulle postazioni desktop le notifiche permangono sulla barra laterale (Fig 2 **B**) finché le cause di inaffidabilità non siano rimosse e il Sistema sia di nuovo affidabile. In tutti i letti coinvolti nell'inaffidabilità, non sono visualizzati dati-paziente finché il Sistema non è di nuovo affidabile.

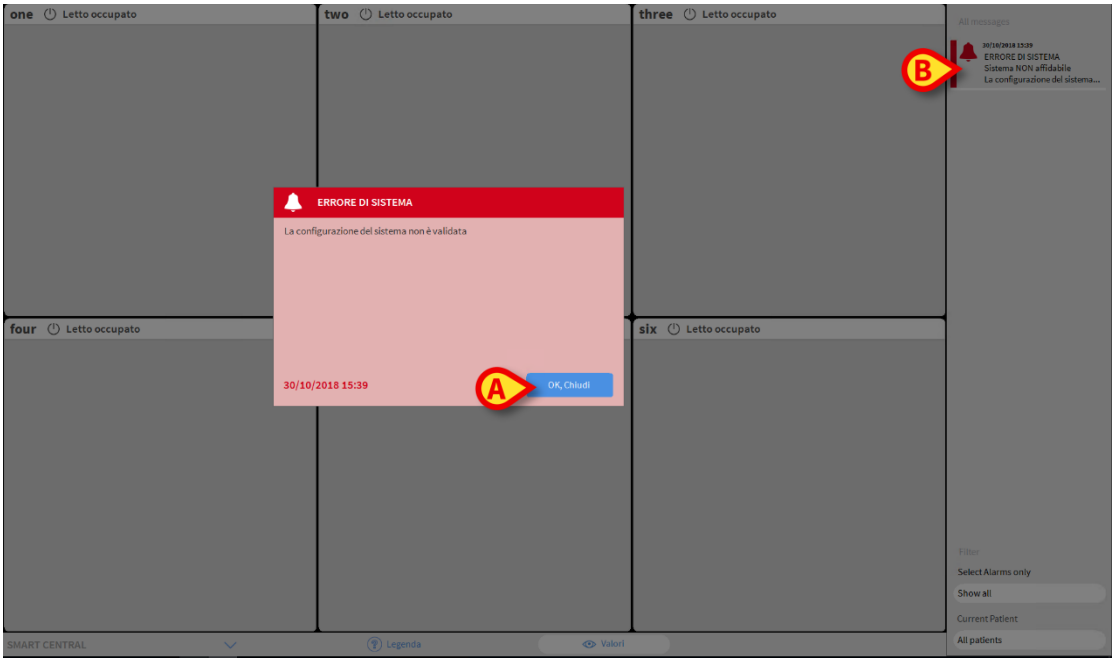


Fig 2 - Sistema non affidabile (desktop)

- Cliccare su **Ok, Chiudi** sulla notifica per indicare la presa visione (Fig 2 **A**).

4.5.2 Mobile

Sui dispositivi portatili è fornita una notifica di "Errore di Sistema". Un allarme sonoro con vibrazione è inoltre attivato.

- Scorrere la notifica verso il basso per presa visione. Ciò ferma l'allarme sonoro e la vibrazione.

Rimane un avvertimento in alto, su ogni schermata del portatile, finché le cause di inaffidabilità siano rimosse e il sistema divenga nuovamente affidabile. In tutti i letti coinvolti nell'inaffidabilità, non sono visualizzati dati-paziente finché il Sistema non è di nuovo affidabile.

4.5.3 Cause di inaffidabilità

In caso di inaffidabilità del Sistema viene notificato un allarme tecnico. L'allarme è una notifica di "Errore di sistema", che fornisce anche una breve descrizione delle cause dell'inaffidabilità.
Le possibili cause di inaffidabilità sono le seguenti:

"La configurazione del Sistema non è validata."
"Smart Central non sta funzionando correttamente. Contattare gli amministratori del Sistema."
"Errore di connessione della torretta luminosa ({0})."
"Timeout ella risposta sul Sistema esterno CDAS. "
"Sistema esterno CDAS disconnesso."
"Errore di accesso al database."
"Anomalia nel componente {0} ({1})."
"Il componente {0} ({1}) non risponde."
"Il driver {0} su {1} non risponde."
"Testo libero inviato dal driver del dispositivo."

I caratteri "{0} e {1}" rappresentano il nome del componente effettivo.

In caso di "Errore di Sistema" in tutti i letti coinvolti non sono visualizzati dati del paziente finché il Sistema non sia di nuovo affidabile.

4.6 Indisponibilità delle postazioni di lavoro

Nel caso in cui la postazione di lavoro (inclusi dispositivi mobili) dove il Prodotto è installato incontri problemi in fase di connessione col server, viene mostrata una apposita schermata.

Se la rete non rispetta le caratteristiche richieste si ha un rallentamento progressivo nel prodotto fino ad arrivare ad errori di time-out sull'accesso ai dati; ciò fino ad entrare in modalità "Recovery".

Il Prodotto tenta un ripristino automatico. Se il ripristino automatico fallisce, è necessario contattare l'assistenza tecnica. Si veda il paragrafo 9 per l'elenco di contatti Ascom UMS.

L'organizzazione ospedaliera che usa il Prodotto è tenuta a definire una procedura di emergenza da attuare in caso di indisponibilità del Prodotto. Ciò al fine di

1. Permettere ai reparti di continuare a svolgere le proprie attività
2. Ripristinare al più presto la disponibilità del Prodotto.

Ascom UMS o il Distributore di riferimento sono disponibili per fornire pieno supporto nella definizione di tale procedura. Si veda il paragrafo 5 per l'elenco dei contatti.

Le funzionalità e le caratteristiche descritte nei paragrafi 4.4 e 4.5 sono applicabili anche quando il Prodotto non è installato e configurato per la distribuzione primaria degli allarmi. Cioè: quando il protocollo di comunicazione dei dispositivi medici non è destinato a questo scopo.
In questi casi le caratteristiche e le funzionalità descritte sopra funzionano come meccanismo di sicurezza addizionale e ridondante che supervisiona i componenti del Prodotto. Possono o non possono supervisionare il collegamento con i dispositivi medici, a seconda della configurazione del Prodotto e delle caratteristiche tecniche del dispositivo medico.

In tali condizioni l'intero sistema non può essere considerato "single fault safe" e non può essere usato come sistema primario di comunicazione affidabile ("reliable") di allarmi.

5. Contatti

Ascom (Solution) AG, Gewerbepark Hintermättlistrasse, 5506 MÄGENWIL, Switzerland

Si faccia riferimento, per qualsiasi comunicazione, al Distributore che ha installato il Prodotto.

Contatti del fabbricante:

Ascom UMS srl unipersonale
Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italia
Tel. (+39) 055 0512161
Fax (+39) 055 8290392

Assistenza tecnica
support.it@ascom.com
800999715 (numero gratuito, valido solo per l'Italia)

Informazioni commerciali
it.sales@ascom.com

Informazioni generali
it.info@ascom.com