Digistat® Produkt Benutzerhandbuch

Revision 1.0

2019-06-11

ASCOM UMS s.r.l. Unipersonale

Via Amilcare Ponchielli Nr. 29, 50018, Scandicci (FI), Italien

Tel. (+39) 055 0512161 – Fax (+39) 055 829030

www.ascom.com

Digistat® Version 6.0

Digistat® wird von der Ascom UMS srl hergestellt (http://www.ascom.com).

Das Produkt Digistat® ist CE gemäß der Richtlinie 93/42/EWG (“Medizinische Geräte”), geändert von der Richtlinie 2007/47/EG, gekennzeichnet.

Ascom UMS ist zertifiziert nach den Standard EN ISO 13485:2016 mit folgendem umfang: “Product and specification development, manufacturing management, marketing, sales, production, installation and servicing of information, communication and workflow software solutions for healthcare including integration with medical devices and patient related information systems”.

Software-Lizenz

Das Produkt darf nur nach Erhalt einer gültigen Lizenz von Ascom UMS oder dem Vertriebspartner verwendet werden.

Lizenzen sind eingetragene warenzeichen

Inhaltsverzeichnis

1. Verwendung des Handbuchs

Dieses Benutzerhandbuch muss in Kombination mit den unten aufgeführten, modulspezifischen Handbüchern verwendet werden. Informationen zu den in der Organisation des Gesundheitswesens verwendeten Digistat-Modulen finden Sie in den entsprechenden Handbüchern:

USR DEU Controlbar
USR DEU Smart Central
USR DEU Smart Central Mobile
USR DEU Vitals Mobile
USR DEU Voice Notes Mobile
USR DEU Identity Mobile
USR DEU Collect Mobile

1.1 Ziele

Bei der Erstellung dieses Handbuches wurde angestrebt, alle notwendigen Informationen zu geben, um einen sicheren und richtigen Gebrauch des Digistat®-Produkts abzusichern und die Identifizierung des Herstellers zu ermöglichen. Außerdem hat dieses Dokument das Ziel, alle einzelnen Teile des Digistat® Produkts zu beschreiben, eine Kurzanleitung für Benutzer, die wissen möchten, wie ein bestimmter Vorgang ausgeführt wird, sowie eine Anleitung für den richtigen Gebrauch des Produkts zu bilden, so dass ein falscher und möglicherweise gefährlicher Gebrauch vermieden werden kann.

1.2 Verwendete Zeichen und Terminologie

Die Verwendung von Digistat® Produkten erfordert eine grundlegende Kenntnis der gebräuchlichsten IT-Begriffe und -Konzepte. Auf die gleiche Weise sind derartige Kenntnisse zum Verständnis dieses Handbuchs notwendig.

Beachten Sie, dass die Verwendung von Digistat® Produkten nur durch beruflich qualifiziertes und entsprechend geschultes Personal erfolgen darf.

1.2.1 Konventionen

In diesem Dokument werden folgende Konventionen verwendet:

- Bezeichnungen von Schaltflächen, Menübefehlen, Optionen, Symbolen, Feldern und allen Elementen der Benutzeroberfläche, mit denen der Nutzer interagieren kann (entweder berühren, anklicken oder auswählen), sind **fett** formatiert.
- Bezeichnungen/Überschriften von Bildschirmen, Fenstern und Registerkarten werden mit „doppelten Anführungszeichen” angegeben.
- Der Programmcode ist in Courier formatiert.
- Das ➢ Aufzählungszeichen gibt eine Aktion an, die der Benutzer durchführen muss,

um eine bestimmte Tätigkeit auszuführen.

- Verweise auf externe Dokumente sind *kursiv* formatiert.

1.3 Symbole

In diesem Handbuch werden die folgenden Symbole verwendet.

	**Nützliche Information** Dieses Symbol erscheint heben zusätzlichen Informationen bezüglich der Eigenschaften und der Verwendung von Digistat®. Dies können erläuternde Beispiele, alternative Abläufe oder jegliche "zusätzlichen" Informationen sein, die für ein besseres Verstehen des Produktes als nützlich angesehen werden.

	**Vorsicht!** Dieses Symbol wird verwendet, um Informationen hervorzuheben, die auf die Vermeidung eines falschen Gebrauchs der Software abzielen oder die Aufmerksamkeit auf kritische Abläufe lenken, die Gefahren hervorrufen können. Demzufolge ist es notwendig, bei jedem Erscheinen des Symbols achtzugeben.

Die folgenden Symbole werden in der Digistat® About-Box verwendet:

	Name und Adresse des Herstellers
	Achtung, begleitende Unterlagen beachten

1.3.1 Digistat About-Box

Die Schaltfläche "Info" im Digistat-Hauptmenü zeigt ein Fenster mit Informationen zur installierten Digistat-Version und den zugehörigen Lizenzen an (Abb. 1). Weitere Informationen finden Sie im Digistat Control Bar-Benutzerhandbuch

Abb. 1

2. Einführung zu Digistat

Die Suite klinischer Module Digistat ist ein fortschrittliches Software-System zur Verwaltung von Patientendaten, das speziell für die Verwendung durch Klinikärzte, Krankenschwestern und Verwalter entworfen wurde.

Das Software-Paket umfasst eine Reihe von Modulen, die entweder allein arbeiten oder vollständig integriert werden, um eine komplette Lösung zur Verwaltung von Patientendaten zu bereitzustellen.

Von der Intensivstation zur Station, vom Operationssaal zur Verwaltungsabteilung, kann Digistat in einem breiten Bereich von Umgebungen verwendet werden.

Die modulare Architektur und die umfangreichen Möglichkeiten zur kundenspezifischen Anpassung von Digistat erlauben es Ihnen, Ihr eigenes System zur Verwaltung von Patientendaten aufzubauen und das System zu erweitern, damit es bei Bedarf Ihren neuen Erfordernissen gerecht wird.

Auf das Digistat Produkt kann nur durch Eingabe von Benutzername und Kennwort zugegriffen werden. Jeder Benutzer wird durch ein detailliertes Profil definiert und kann nur auf die ihm erlaubten Bereiche zugreifen. Vom Produkt wird automatisch eine Aufzeichnung aller ausgeführten Vorgänge angelegt.

2.1 Modulare Architektur

“Modulare Architektur” bedeutet, dass verschiedene Anwendungssoftware (oder Module) mit bestimmten Zwecken in der gleichen Software-Umgebung (Digistat in diesem Fall) implementiert werden können, die durch eine bestimmte graphische Gestaltung, allgemeine Zwecke und Nutzungsbedingungen gekennzeichnet ist.
Verschiedene Module können zu unterschiedlichen Zeitpunkten auf eine Weise hinzugefügt werden, die mit dem Benutzer abgestimmt wird. Die dabei entstehende Software-Suite entspricht den spezifischen Erfordernissen des Benutzers und kann entsprechend der möglichen Änderungen bei den Bedürfnissen des Benutzers rechtzeitig geändert werden.

2.2 Beabsichtigter Gebrauch

Die Software Digistat (nachstehend kurz als "Produkt" bezeichnet) erfasst, registriert, organisiert, sendet und zeigt Informationen und Daten des Patienten an, einschließlich der Daten und Ereignisse, die aus den angeschlossenen medizinischen Systemen und Geräten übernommen werden, und der eventuell von Hand eingegebenen Informationen, um das klinische Personal bei der Diagnose und Behandlung der Patienten zu unterstützen und eine elektronischen Krankenkartei anzulegen.

- Das Produkt erstellt eine elektronische, konfigurierbare Dokumentation des Patienten, die sowohl auf den eingegebenen Daten und Informationen beruht, als auch auf der automatischen und manuellen Dokumentation der Aktivität der Abteilung.

- Das Produkt bietet eine sekundäre, automatische Anzeige und akustische Information über erfasste Daten, Ereignisse, laufenden Zustand und Betriebsbedingungen der angeschlossenen medizinischen Systeme und Geräte auf eigenen Anzeigegeräten. Das Produkt kann auch so konfiguriert werden, dass es Daten und Informationen zu Ereignissen, Zuständen und Betriebsbedingungen an das Nachrichtensystem von Ascom weiterleitet.
- Das Produkt unterstützt die Verbesserung der Arbeitsabläufe des Pflegepersonals in Bezug auf das Management der Alarme, die von den angeschlossenen medizinischen Systemen und Geräten gegeben werden.
- Das Produkt unterstützt die Dokumentation der verschriebenen Behandlung, ihrer Vorbereitung und ihrer Ausführung.
- Das Produkt unterstützt die Aufzeichnung, Überprüfung und Anzeige von Vitalwerten in Diagrammen basierend auf den erfassten Daten und Informationen.
- Das Produkt erstellt konfigurierbare Berichte, Diagramme und Statistiken basierend auf aufgezeichneten Daten zur Verwendung durch das medizinische Personal, um die Effizienz, Produktivität, Leistung und Ressourcen-Verwendung sowie die Qualität der Pflege zu analysieren.

Das Produkt ist **kein** Ersatz oder Wiederholung der primären Anzeige der Daten und der Alarme der angeschlossenen Systeme und Geräte, und hat **keine** Kontrolle, Überwachung oder Einfluss auf die genannten Systeme und Geräte noch auf die damit verbundenen Alarmmeldungen.

Das Produkt ist **nicht** zur Verwendung als Instrument für direkte Diagnose oder Überwachung der lebenswichtigen physiologischen Parameter bestimmt.

Das Produkt ist für den Einsatz im Klinik-/Krankenhausbereich durch entsprechend ausgebildete Fachleute der Gesundheitsbranche bestimmt und basiert auf der korrekten Nutzung und dem Betrieb der Datenverarbeitungs- und Kommunikationsinfrastruktur, die im jeweiligen Institut bereits vorhanden sind, sowie auf der korrekten Nutzung und dem Betrieb der vorhandenen Anzeigegeräte und der angeschlossenen medizinischen Systeme und Geräte.
Außerdem bietet das Produkt spezielle Funktionen und Schnittstellen zur Verwendung durch nicht berufsmäßige rechnerferne Benutzer zur Anzeige von Informationen, Berichte, Diagramme und Statistiken, ohne dass diese die Möglichkeit zur Hinzufügung, Änderung oder Löschung von Informationen oder Daten haben.

Das Produkt ist eine Standalone-Software, die auf Servern und Computern installiert wird, deren Hardware und Software den technischen Spezifikationen entsprechen müssen, die dem Produkt mitgeliefert werden.

2.2.1 Sicherheitshinweise

Der Benutzer darf seine therapeutischen und diagnostischen Entscheidungen und Eingriffe ausschließlich nach direkter Überprüfung der primären Informationsquelle treffen. Die Kontrolle der Korrektheit der vom Produkt gelieferten Informationen, sowie deren sachgerechte Anwendung liegt ausschließlich in der Verantwortung des Benutzers.

Nur von autorisierten Berufsärzten digital oder Papierausdruck gegengezeichnete Angaben dürfen als gültige klinische Dokumentation betrachtet werden. Die Unterschrift des Benutzers auf den genannten Ausdruck bestätigt, dass er die im Dokument enthaltenen Informationen auf ihre Richtigkeit und Vollständigkeit hin überprüft hat.

Bei der Eingabe patientenbezogener Daten ist der Benutzer dafür verantwortlich, zu überprüfen, ob die Patientenidentität, die Abteilung/Pflegeeinheit der Gesundheitseinrichtung und die Bettenangaben im Produkt korrekt sind. Diese Kontrolle ist von ausschlaggebender Wichtigkeit bei kritischen Vorgängen, wie beispielsweise die Verabreichung von Arzneimitteln.

Die Gesundheitseinrichtung ist dafür verantwortlich, geeignete Verfahren zu identifizieren und umzusetzen, um sicherzustellen, dass am und/oder bei der Benutzung des Produkts aufgetretene Fehler schnell erkannt und berichtigt werden, und dass sie weder für den Patienten noch den Benutzer ein Risiko darstellen. Diese Verfahren hängen von der Konfiguration des Produkts und der von der Gesundheitseinrichtung bevorzugten Verwendungsmethode ab.

Das Produkt kann je nach Konfiguration Zugang zu Informationen über die Arzneimittel geben. Die Gesundheitseinrichtung ist dafür verantwortlich, zu Beginn und im Anschluss regelmäßig zu überprüfen, dass diese Informationen aktuell und aktualisiert sind.

Das Produkt hat keine primäre Benachrichtigungsfunktion über Warnmeldungen und ist nicht zur Verwendung als Ersatz der direkten Überwachung der von den medizinischen Geräten erzeugten Warnmeldungen vorgesehen.

Diese Einschränkung ist neben anderen Gründen durch die Spezifikationen und Beschränkungen der Kommunikationsprotokolle der medizinischen Geräte bedingt.
Sofern sich einige der für das Produkt verwendeten Geräte innerhalb des Patientenbereichs befinden oder an Vorrichtungen angeschlossen sind, die sich innerhalb des Patientenbereichs befinden, muss die Gesundheitseinrichtung ist dafür verantwortlich, dass die gesamte kombinierte Anwendung der internationalen Norm IEC 60601-1 und allen zusätzlichen Anforderungen der örtlichen Vorschriften entspricht.

Bei der Verwendung des Produkts muss eine spezifische Konfiguration der Benutzerkonten und aktive Überwachung gewährleistet sein: 1) die aufgrund der Produktangaben durch Personal des Herstellers oder dessen Händler eingewiesen

wurden und 2) beruflich für die korrekte Auslegung der vom Produkt gelieferten Informationen und zur Anwendung der geeigneten Sicherheitsabläufe qualifiziert sind.

Das Produkt ist eine eigenständige Software, die auf Standardcomputern und/oder mobilen Standardgeräten ausgeführt wird, die mit dem lokalen Netzwerk der Gesundheitseinrichtung verbunden sind.

Die Gesundheitseinrichtung ist dafür verantwortlich, Computer, Geräte und lokale Netzwerke ausreichend vor Cyber-Angriffen zu schützen.

Das Produkt darf nur auf Computern und Geräten installiert werden, deren Hardware die Mindestanforderungen erfüllt und nur auf den vom Produkt unterstützten Betriebssystemen.

2.3 Zulassungsüberschreitende (Off-label) Anwendung des Produkts

Jede Anwendung des Produkts außerhalb der als Bestimmungszweck angegebenen Bereiche (im gängigen Sprachgebrauch als „off-label“ bezeichnet), steht vollständig im Ermessen und in der Verantwortlichkeit des Anwenders und der verantwortlichen Organisation.

Der Hersteller kann in keiner Weise die Sicherheit und die Eignung des Produkts gewährleisten, wenn es außerhalb der als Bestimmungszweck angegebenen Bereiche verwendet wird.

Das Produkt **ist kein** primäres verteiltes Alarmsystem.

2.4 Patientenpopulation

Das Produkt ist eine Softwareanwendung und steht nicht in Kontakt mit dem Patienten. Die Patientengruppe und die Patientenbedingungen werden durch die Medizingeräte und -systeme bestimmt, an die das Produkt angeschlossen ist.
Zusätzlich gelten folgende Anforderungen:

- Patientengewicht zwischen 0,1 kg und 250 kg
- Patientenhöhe zwischen 15cm und 250cm

2.5 Verantwortlichkeiten der Organisation des Gesundheitswesens

Ascom UMS haftet nicht für die Auswirkungen auf die Sicherheit und Effizienz der Einrichtung von Reparatur- oder Wartungsarbeiten, die nicht vom Personal des eigenen Kundendienstes bzw. von Ascom UMS oder deren Vertragshändlern autorisierten Fachtechnikern ausgeführt wurden.

Der Benutzer und die rechtlich verantwortlichen Personen der Organisation des Gesundheitswesens, in der das Gerät verwendet wird, werden auf die Verantwortlichkeit hingewiesen, die ihnen aufgrund der einschlägigen

Gesetzesvorschriften für die Sicherheit am Arbeitsplatz (GvD Nr. 81 vom 09.04.2008) sowie der Aufsichtspflicht vor Ort zur Vermeidung von gefährlichen oder potentiell gefährlichen Unfällen zukommt.

Der Kundendienst der Fa. Ascom UMS und ihrer Vertragshändler ist in der Lage, den Kunden die notwendige Unterstützung zu bieten, um die Sicherheit und Funktionstüchtigkeit der gelieferten Geräte über der Zeit aufrecht zu erhalten. Er gewährleistet Fachkompetenz und Ausstattung mit den nötigen Gerätschaften und Ersatzteilen, um sicherzustellen, dass die Geräte langfristig in vollem Umfang den ursprünglichen Spezifikationen des Herstellers entsprechen.

Das Produkt wurde unter Berücksichtigung der Anforderungen und Best Practices der Norm IEC 80001 und ihrer technischen Begleitberichte entwickelt. Insbesondere IEC/TR 80001-2-5:2014 hat eine große Relevanz für das Produkt. Wie bei der Produktreihe IEC 80001 geklärt, unterliegt ein Teil der notwendigen Aktivitäten und Risikokontrollmaßnahmen der Kontrolle und Verantwortung der verantwortlichen Organisation. Bitte beziehen Sie sich auf die Normen und ihre Sicherheiten, um die erforderlichen Aktivitäten und Maßnahmen zur Risikokontrolle zu ermitteln; insbesondere verweisen wir auf die folgenden Dokumente:

- IEC 80001-1:2010
- IEC/TR 80001-2-1:2012
- IEC/TR 80001-2-2:2012
- IEC/TR 80001-2-3:2012
- IEC/TR 80001-2-4:2012
- IEC/TR 80001-2-5:2014

2.6 Verantwortlichkeit des Herstellers

Ascom UMS betrachtet sich für die Sicherheit, die Zuverlässigkeit und die Leistungen des Produkts nur dann verantwortlich, wenn:

- Die Installation und Konfiguration erfolgte durch von Ascom UMS geschultes und autorisiertes Personal;
- Verwendung und Wartung entsprechen den Anweisungen in der Produktdokumentation (einschließlich dieser Bedienungsanleitung);
- Konfigurationen, Änderungen und Wartungen werden nur durch von Ascom UMS ausgebildetes und autorisiertes Personal durchgeführt;
- Die Einsatzumgebung des Produkts entspricht den geltenden Sicherheitshinweisen und Vorschriften;
- Die Umgebung, in der das Produkt verwendet wird (einschließlich Computer, Geräte, elektrische Anschlüsse usw.), entspricht den geltenden lokalen Vorschriften.

Ist das Produkt Teil eines "medizinischen elektrischen Systems" durch elektrische und funktionelle Verbindung mit medizinischen Geräten, ist die Gesundheitsorganisation für die erforderlichen elektrischen Sicherheitsüberprüfungen und Abnahmen zuständig, auch wenn Ascom UMS die erforderlichen Verbindungen ganz oder teilweise durchgeführt hat.

2.7 Rückverfolgbarkeit des Produkts

Um die Rückverfolgbarkeit der Geräte zu gewährleisten und Korrekturmaßnahmen vor Ort durchzuführen, muss der Eigentümer gemäß EN 13485 und MDD 93/42/EWG Ascom UMS/den Vertriebspartner über jede Eigentumsübertragung informieren, indem er das Produkt, den früheren Eigentümer und die Identifikationsdaten des neuen Eigentümers schriftlich mitteilt.
Gerätedaten finden Sie auf dem Produkt-Label (das Feld „Info“ wird im Produkt angezeigt – siehe Seite **Error! Bookmark not defined.**).
Bei Zweifeln/Fragen zur Produktidentifikation wenden Sie sich bitte an den technischen Kundendienst von Ascom UMS/des Vertriebspartners (Ansprechpartner siehe Seite **Error! Bookmark not defined.**).

2.8 After-Sales-Aufsichtssystem

Das mit CE gekennzeichnete Gerät unterliegt einer Überwachung nach dem Inverkehrbringen auf tatsächliche und potenzielle Risiken entweder für den Patienten oder für den Benutzer während des Produktlebenszyklus, die Ascom UMS und sein Vertriebshändler für jede vermarktete Kopie bereitstellen.
Bei einer Verschlechterung der Geräteeigenschaften, schlechter Leistung oder unzureichender Benutzeranweisungen, die entweder die Gesundheit des Patienten oder des Benutzers gefährden oder die Umwelt gefährden könnten, muss der Benutzer unverzüglich Ascom UMS oder den Vertriebshändler benachrichtigen.
Nach Erhalt eines Benutzerfeedbacks wird Ascom UMS/der Vertriebshändler sofort den Überprüfungs- und Verifizierungsprozess starten und die erforderlichen Korrekturmaßnahmen durchführen.

2.9 Standzeit des Produkts

Die Lebensdauer des Produkts hängt nicht von dem Tragen oder anderen Faktoren ab, die die Sicherheit beeinträchtigen könnten. Sie wird durch die Veralterung der Softwareumgebung (z. B. Betriebssystem,NET Framework) beeinflusst und ist daher auf 5 Jahre ab dem Veröffentlichungsdatum der Produktversion (im Feld Info verfügbar) festgelegt.

3. Software/Hardware spezifikationen

Digistat darf nur von geschultem Fachpersonal installiert werden. Dies gilt auch für das Personal von Ascom UMS/Distributoren und jede andere Person, die von Ascom UMS/Distributor speziell geschult und ausdrücklich autorisiert wurde. Ohne die ausdrückliche, direkte Genehmigung von Ascom UMS/Distributor sind Mitarbeiterl der Gesundheitsorganisation nicht berechtigt, Installationsvorgänge durchzuführen und/oder die Digistat-Konfiguration zu ändern.

Digistat darf nur von geschultem Personal verwendet werden. Digistat kann nicht ohne eine entsprechende Schulung durch Ascom UMS/Distributoren verwendet werden.

In diesem Kapitel sind die Software- und Hardware-Merkmale aufgeführt, die für den einwandfreien Betrieb des Produkts notwendig sind. Die in diesem Abschnitt gelieferten Informationen erfüllen die Informationspflicht des Herstellers laut Norm IEC 80001-1:2010 („Application of risk management for IT-networks incorporating medical devices“).

Wenn elektrische Geräte in der Nähe des Bettes aufgestellt werden, müssen aufgrund der Norm IEC 60601-1 medizintechnisch geeignete Geräte verwendet werden. Normalerweise werden in solchen Umgebungen medizintechnisch geeignete PC-PANELS eingesetzt. Bei Bedarf kann Ascom UMS mögliche Geräte dieser Art empfehlen.

Auf dem Arbeitsplatzrechner muss ein entsprechender PDF-Reader installiert sein, um die Online-Hilfe anzuzeigen. Siehe 3.1.3 Softwareanforderungen für zentrale & bettseitige Arbeitsplatzrechner.

3.1 Bettseitig

3.1.1 Hardware

Mindestanforderungen an die Hardware:

- Prozessor Intel® I3 oder höher
- RAM- Speicher 4GB
- Festplatte mit mindestens 60 GB freiem Speicherplatz
- Monitor mit Auflösung 1024 x 768 oder höher (empfohlen 1920 x 1080)
- Maus oder kompatibles Gerät
- Ethernet- Schnittstelle 100 Mb/s (oder höher)
- CD/DVD-Reader oder andere Möglichkeit, die Installationsdateien zu kopieren

Für den Fall, dass eine Zentrale oder eine Workstation am Krankenbett für die Anzeige von Videostreams konfiguriert ist (Funktion wird nur in Smart Central oder OranJ mit aktivierter Kameraintegration unterstützt), gelten die folgenden Mindestanforderungen::

- Intel® I3 Prozessor (oder schneller)
- Speicher: 4 GB RAM + 50 MB für jeden gleichzeitig angezeigten Kamerastream (z. B. bei 20 angezeigten Kameras 4 GB + 1 GB)
- Festplatte: mindestens 60 GB verfügbarer Speicherplatz
- Monitor: 1024 x 768 oder höher (1920 x 1080 empfohlen)
- Maus oder anderes kompatibles Gerät
- Ethernet-Schnittstelle 100 Mb / s (oder höher)
- CD / DVD-Laufwerk oder Möglichkeit zum Kopieren der Installationsdateien

Einige Beispiele: Mit Intel i7 6600 2,60 GHz und einem Streaming von 10 Kameras mit einer Bitrate von 3138 Kbit/s liegt die CPU-Auslastung bei etwa 45 %. Mit I3 7100t 3,4 GHz und einem Streaming von 16 Kameras mit einer Bitrate von 958 Kbit/s liegt die CPU-Auslastung bei etwa 30 %.

3.1.2 Betriebssystem

- Microsoft Corporation Windows 7 SP1 x86/x64 Professional
- Microsoft Corporation Windows 8.1 x86/x64 Professional
- Microsoft Corporation Windows 10

3.1.3 System Software

- Microsoft Framework .NET 4.5
- Adobe Acrobat Reader 10

HINWEIS: Das Produkt-Benutzerhandbuch ist eine PDF-Datei, die nach dem PDF-Standard Version 1.5 erstellt wurde und somit von Adobe Acrobat 6.0 oder höher lesbar ist. Darüber hinaus wurde das Produkt-Benutzerhandbuch mit Adobe Acrobat Reader 10 getestet. Der Betreiber des Krankenhauses kann ggf. eine andere Version des Acrobat Reader verwenden: Die Überprüfung des installierten Produkts beinhaltet die Überprüfung der korrekten Lesbarkeit des Benutzerhandbuchs.

3.2 Server

3.2.1 Hardware

Minimale Hardwareanforderungen (kleine Installation, 20 Betten, jeweils 4 Geräte):

- Intel® I5 Prozessor mit 4 Kernen.
- RAM- Speicher 4 GB (empfohlen 8 GB)
- Festplatte mit mindestens 120 GB freiem Speicherplatz
- Ethernet- Schnittstelle 100 Mb/s (oder höher). Empfohlen 1 Gb/s.

- CD/DVD-Reader oder andere Möglichkeit, die Installationsdateien zu kopieren

Empfohlene Hardwareanforderungen (mittelgroße Installation, 100 Betten, jeweils 4 Geräte, Connect und Mobile):):

- Intel® I7 Prozessor mit 8 Kernen.
- RAM- Speicher: 32 GB RAM.
- Festplatte mit mindestens 120 GB freiem Speicherplatz
- Ethernet- Schnittstelle: 1 Gb/s.
- CD/DVD-Reader oder andere Möglichkeit, die Installationsdateien zu kopieren

3.2.2 Betriebssystem

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016

3.2.3 System Software

- Microsoft SQL Server 2008R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft Framework.NET 4.5

3.3 Digistat “Mobile”

Digistat Mobile (nachfolgend „Digistat Mobile“) wurde auf dem Gerät Ascom Myco SH1 und SH2 Wi-Fi und mobile Smartphone-Geräte, mit Version Android 4.4.2 (Myco1) oder 5.1 (Myco1/Myco2) oder 8.0 (Myco3) getestet. Die Anwendung ist daher kompatibel mit Myco1, Myco2 und Myco3.

Die Anwendung ist so konzipiert, dass sie mit anderen Android-Geräten mit einer Mindestbildschirmgröße von minimum 3,5 Zoll kompatibel ist. Die Kompatibilität mit einem bestimmten Gerät muss vor dem klinischen Einsatz überprüft werden.

Wenden Sie sich bitte an Ascom UMS/Vertriebshändler, um eine Liste der verfügbaren Treiber zu erhalten.

3.4 Digistat “Web”

Die folgenden Browser werden für die Verwendung mit Digistat-Webanwendungen unterstützt:

- Chrome 63
- Firefox 56
- Edge 41
- Internet Explorer 11

	Für Digistat Web sollten nur unterstützte Webbrowser verwendet werden.
	Eine Digistat Web-Workstation wird immer den Webbrowser im Vordergrund haben. Außerdem darf der Web-Browser niemals für etwas anderes als Digistat Web verwendet werden (was auch bedeutet, dass die Digistat Web-Homepage die Standard-Homepage des Web-Browsers sein soll).
	Die Anzeige-Skalierung des Browsers muss immer auf 100% eingestellt sein.
	Wenn das lokale Netzwerk zumindest teilweise auf Wi-Fi-Verbindungen basiert, kann es aufgrund der intermittierenden Art von Wi-Fi-Verbindungen zu Unterbrechungen kommen, die den Getrennten Modus aktivieren (grauer Teppich, der Digistat Web abdeckt) und somit möglicherweise nicht verfügbar ist. Die Organisation des Gesundheitswesens muss funktionieren, um eine optimale WLAN-Abdeckung sicherzustellen und die Mitarbeiter darüber zu informieren, wie diese vorübergehenden Produktausfälle zu behandeln sind.

3.5 Allgemeine Warnungen

	Die im entsprechenden Benutzerhandbuch vorgestellte Anwendung „MDI Web“ kann nur zu Demonstrationszwecken verwendet werden. Sie kann nicht in einer Produktionsumgebung verwendet werden.
	Zur korrekten Verwendung von dem Produkt muss das Display Scaling von Microsoft Windows auf 100% eingestellt sein. Abweichende Einstellungen können die Ausführung des Produkts verhindern oder Störungen der grafischen Darstellung hervorrufen. Zur Einstellung des Werts Display Scaling bitte die Dokumentation von Microsoft Windows nachschlagen.
	Die vertikale Mindestauflösung von 768 wird nur unterstützt, wenn dem Produkt für Full-Screen-Ausführung konfiguriert ist oder wenn die Anzeigeleiste von Windows auf automatisches Ausblenden (Auto-Hide) eingestellt ist.
	Die Computer und die anderen verwendeten Einrichtungen müssen für die Umgebung geeignet sein, in der sie eingesetzt werden sollen und müssen daher die relevanten Normen und Vorschriften einhalten.
	Bei Lagerung, Transport, Installation, Wartung und Entsorgung von Hardware Dritter müssen obligatorisch die Angaben des Herstellers eingehalten werden. Die genannten Vorgänge dürfen ausschließlich von Fachpersonal bzw. entsprechend geschultem Personal ausgeführt werden.
	Die Verwendung des Produkts zusammen mit einer beliebigen anderen Software als der in diesem Dokument vorgegebenen, kann die Sicherheit, Funktionstüchtigkeit und die Ausführungskontrollen des Produktes beeinträchtigen. Eine derartige Verwendung kann zu einem höheren Risiko für Anwender und Patienten führen. Es ist unbedingt erforderlich, einen zugelassenen Techniker von Ascom UMS oder dem Händler zu konsultieren, bevor mit dem Produkt eine andere Software verwendet werden kann, als die in diesem Dokument angegebene. Sollte die Hardware, auf der das Produkt betrieben wird ein unabhängiger Computer sein, darf der Anwender keinerlei andere Software (Dienst- oder Anwendungsprogramme) auf dem Computer installieren. Es wird geraten, mit einer einzuführenden Genehmigungspolitik zu verhindern, dass die Anwender Vorgänge, wie die Installation neuer Software, ausführen.

	Die verantwortliche Organisation ist gehalten auf den Workstations, auf denen Produkt betrieben wird, einen Mechanismus zur Synchronisation von Datum und Uhrzeit mit einer Referenz-Uhr zu implementieren.
	Es wird empfohlen, den Internetzugang auf den Client-Workstations und den Handheld-Geräten, auf denen das Produkt verwendet wird, zu deaktivieren. Alternativ soll die Gesundheitsorganisation die notwendigen Sicherheitsmaßnahmen ergreifen, um einen angemessenen Schutz vor Cyber-Angriffen und der Installation nicht autorisierter Anwendungen zu gewährleisten.
	Teile des Produkts fungieren als Viewer von Videostreams. Das Produkt ist nicht die Quelle des Videostreams und zeichnet diese Informationen in keiner Weise auf. Die Organisation des Gesundheitswesens ist dafür verantwortlich, das System aus datenschutzrechtlicher Sicht zu verwalten, einschließlich der Installation und Konfiguration von Quellkameras.
	Teile des Produkts verarbeiten Audio- und Bilddaten, die sich auf Benutzer und/oder Patienten beziehen, einschließlich Erfassung, Ausarbeitung und Aufzeichnung. Es liegt in der Verantwortung der Organisation des Gesundheitswesens, die erforderlichen Verfahren zur Einhaltung der örtlichen Datenschutzbestimmungen umzusetzen. Einschließlich, aber nicht beschränkt auf die Definition von Nutzungsgrenzen und die Schulung von Benutzern.
	Die Video-Streaming-Funktionalität auf Desktop-Workstations wurde mit den Video-Codecs H264 und H265 getestet. Alle anderen Video-Codecs, die von Drittanbieteranwendungen (z. B. VLC Media Player) stammen oder schon vorhanden sind, müssen vor der Verwendung getestet werden.
	Achtung: Jede Videoquelle unterstützt eine maximale Anzahl gleichzeitig verbundener Clients. Es liegt in der Verantwortung der Organisation des Gesundheitswesens, diese maximale Anzahl zu bestimmen und die Benutzer zu informieren.
	Die Video-Streaming-Funktion auf Mobilgeräten unterstützt nur RTSP-Video-Streams mit den folgenden Authentifizierungstypen: • Keine Authentifizierung; • Grundlegende Authentifizierung; • Authentifizierung in Kurzfassung.
	Die Video-Streaming-Funktion auf Mobilgeräten unterstützt nur die Videocodecs H263, H264 und H265.

3.6 Firewall und Antivirus

Zum Schutz des Produkts vor möglichen informatischen Angriffen ist folgendes notwendig:

- der Firewall von Windows muss sowohl an allen Workstations als auch auf dem Server aktiv sein;
- an den Workstations und auf dem Server muss ein Antivirus/Antimalware-Programm installiert sein und regelmäßig aktualisiert werden.

Die Organisation des Gesundheitswesens hat dafür zu sorgen, dass diese beiden Schutzeinrichtungen vorhanden sind. Ascom UMS hat das Produkt mit F-SECURE Antivirus getestet. Es steht der verantwortlichen Organisation jedoch frei, aufgrund der bisherigen Entscheidungen und Politiken im jeweiligen Krankenhaus das spezifische Antivirus-Programm selbst zu wählen. Ascom UMS kann nicht gewährleisten, dass das Produkt mit allen Antivirus-Softwares oder deren Konfigurationen kompatibel ist.

	Bei Verwendung des Antivirus-Programms Kaspersky wurde Unverträglichkeit mit Teilen von Digistat gemeldet, zu deren Lösung die Bestimmung spezifischer Regeln im Antivirus-Programm selbst notwendig war.

	Es wird dringend empfohlen, nur die Ports TCP und UDP offen zu halten, die tatsächlich notwendig sind. Diese können je nach Konfiguration des Produkts variieren. Es empfiehlt sich deshalb, sich an den Kundendienst zu wenden, um von Fall zu Fall die notwendigen Informationen einzuholen.

3.6.1 Weitere empfohlene Vorsichtsmaßnahmen für den Cyberschutz

Um das Produkt vor möglichen Cyber-Angriffen zu schützen, wird dringend empfohlen:

- Planen und implementieren des "Härtens" der IT-Infrastruktur inklusive der IT-Plattform, die die Laufzeitumgebung für das Produkt darstellt,
- Einsatz eines Intrusion Detection and Prevention Systems (IDPS),
- Durchführung eines Penetrationstests und, falls eine Schwachstelle festgestellt wird, Ergreifen aller erforderlichen Maßnahmen, um das Risiko eines Cyber-Eindringens zu minimieren,
- Entfernung der Geräte, wenn sie nicht mehr updatefähig sind,
- Planung und Durchführung einer periodischen Überprüfung der Integrität der Dateien und Konfigurationen,
- Implementierung einer DMZ-Lösung (Demilitarisierte Zone) für Webserver, die auf das Internet zugreifen müssen.

3.7 Eigenschaften des lokalen Netzes

In diesem Abschnitt sind die Eigenschaften beschrieben, die das lokale Netz, an dem das Produkt installiert werden soll aufweisen muss, um die einwandfreie Funktion des Produkts zu gewährleisten.

- Das Produkt verwendet für den Datenverkehr das Standardprotokoll TCP/IP.
- Das LAN- Netz muss frei von Überlastungen und/oder Sättigungen sein.
- Das Produkt ist geeignet für ein LAN- Netz mit 100 Mbps an den Benutzer-Stationen. Empfehlenswert ist das Vorhandensein von Datenhauptleitungen mit 1 Gbps.
- Zwischen den Workstations, dem Server und den Sekundärgeräten dürfen für den Datenverkehr TCP/IP keine Filter vorhanden sein.
- Sofern die Geräte (Server, Workstation und Sekundärgeräte) an andere Teilnetze angeschlossen sind, muss zwischen diesen Teilnetzen ein Routing vorhanden sein.
- Es empfiehlt sich, den Aufbau des Produkts redundant auszuführen, um den Netzbetrieb auch im Störungsfall gewährleisten zu können.
- Darüber hinaus empfiehlt sich eine Absprache bei der Planung der Wartungsmaßnahmen, damit der Vertragshändler das Krankenhaus beim optimalen Management der Leistungsunterbrechungen unterstützen können.

	Sofern das Netz nicht die geforderten Eigenschaften aufweist, arbeitet das Produkt nach und nach langsamer, bis es zu Timeout-Fehlern beim Zugriff auf die Daten und schließlich zum Eintreten der Modalität “Recovery” kommt.
	Sofern ein WiFi-Netz verwendet wird, kann es durch die Schwankungen der WiFi-Verbindung zu kurzzeitigen Unterbrechungen der Netz-Anbindung kommen, so dass der “Recovery Mode” aktiviert wird und das Produkt nicht betriebsfähig ist. Die verantwortliche Organisation muss dafür sorgen, dass eine optimale Deckung und Stabilität des WiFi-Netzes gewährleistet wird. Außerdem muss das davon betroffene Personal informiert werden, wie es sich bei möglichen, kurzzeitigen Unterbrechungen der Netzanbindung zu verhalten hat.
	Um die über drahtlose Netzwerke übertragenen Daten zu verschlüsseln, wird empfohlen, das höchstmögliche Sicherheitsprotokoll zu verwenden; in jedem Fall nicht weniger als WPA2.

3.7.1 Die Auswirkung von dem Produkt auf das Netzwerk des Krankenhauses

Das Produkt wirkt sich auf die Struktur des lokalen Netzwerks des Gesundheitswesens aus. Dieser Abschnitt enthält Informationen zum von dem Produkt im Netzwerk hervorgerufenen Datenverkehr, damit es der Einrichtung möglich ist, die Gefahren in Verbindung mit der Einführung von dem Produkt zu analysieren und beurteilen.

Die von einem Produkt verwendete Datenübertragungsrate ist von vielen verschiedenen Faktoren abhängig. Die wichtigsten davon sind:

- Anzahl der Arbeitsplätze;
- Anzahl der als Zentralstationen konfigurierten Arbeitsplätze;
- Anzahl und Art der zur Datenerfassung dienenden Geräte (entweder nur oder auch dazu dienend);
- Schnittstellen zu externen Systemen;
- Konfiguration und Verwendungsweise von der Produkt

Die Belegung der Produkt-Bandbreite hängt hauptsächlich von der Datenerfassung von medizinischen Geräten ab. In einer Konfiguration mit Erfassung auf 100 Betten, wobei jedes Bett Daten von 1 Ventilator, 1 Patientenmonitor und 3 Infusionspumpen sowie 10 Produkt-Workstations mit je 10 Betten erfasst, die folgenden Werte für die Datenübertragungsrate vorausbestimmt werden.

Durchschnittlich: 0,8 – 6 Mbit/s
Grundfrequenz: 5 – 25 Mbit/s

Bei Produkt-Konfigurationen ohne Erfassung durch medizinische Geräte sind die Bandbreitenbelegungswerte niedriger als die oben angegebenen.

4. Vor dem Start

4.1 Vorschriften für Installation und Wartung

Die nachstehenden Vorschriften für die korrekte Installation und Wartung des Produkts müssen strikt eingehalten werden.

	Wartungs- und Reparaturarbeiten dürfen nur von Ascom UMS/Distributor-Technikern oder von Ascom UMS/Distributor geschultem und autorisiertem Personal in Übereinstimmung mit den Ascom UMS Verfahren durchgeführt werden..

	Es wird empfohlen, dass die Gesundheitsorganisation, die das Produkt verwendet, einen Wartungsvertrag mit Ascom UMS oder einem autorisierten Distributor abschließt. Ein Teil der Wartung umfasst das Upgrade auf die neueste verfügbare Version des Produkts.

Es wird darauf hingewiesen, dass Produkt ausschließlich von geschultem und autorisiertem Personal installiert und konfiguriert werden darf. Dazu gehören das Personal der Fa. Ascom UMS oder der Vertragshändler, sowie alle sonstigen, spezifisch geschulten und von Ascom UMS oder deren Vertragshändlern autorisierten Personen.
Ebenso dürfen Wartungs- und Reparaturarbeiten am Produkt ausschließlich von geschultem und autorisiertem Personal vorgenommen werden, das die entsprechenden Vorschriften und Leitlinien des Herstellers einzuhalten hat. Dazu gehören das Personal der Fa. Ascom UMS oder der Vertragshändler, sowie alle sonstigen, spezifisch geschulten und von Ascom UMS oder deren Vertragshändlern autorisierten Personen.

	Das Produkt darf ausschließlich von geschultem und autorisiertem Personal installiert und konfiguriert werden. Dazu gehören das Personal der Fa. Ascom UMS oder der Vertragshändler, sowie alle sonstigen, spezifisch geschulten und von Ascom UMS oder deren Vertragshändlern autorisierten Personen.

- Ausschließlich genehmigte Einrichtungen mit dem Kennzeichen CE verwenden.
- Es empfiehlt sich, ausschließlich Einrichtungen zu verwenden, die von Ascom UMS bzw. deren Händlern genehmigt wurden. Ohne spezifische Schulung können diese Geräte nicht installiert werden.
- Es empfiehlt sich, ausschließlich Einrichtungen zu verwenden, die von Ascom UMS bzw. deren Händlern genehmigt wurden. Andernfalls besteht die Gefahr, Patienten oder Pflegepersonal zu verletzen.

- Die Vorschriften des Herstellers für die Installation der Hardware müssen strikt eingehalten werden.

- Die interne Speicherplatte muss in regelmäßigen Abständen gewartet und das Betriebsprodukt überprüft werden.

- Die Organisation des Gesundheitswesens ist dafür verantwortlich, Geräte auszuwählen, die für die Umgebung geeignet sind, in der sie installiert und verwendet werden. Die Organisation des Gesundheitswesens sollte unter anderem die elektrische Sicherheit, EMV-Emissionen, Funkstörungen, Desinfektion und Reinigung berücksichtigen. Im Patientenbereich installierte Geräte sind zu beachten

4.2 Vorkehrungen und Warnungen

	Befolgen Sie sorgfältig die Anweisungen in diesem Abschnitt des Handbuchs, um die Zuverlässigkeit und Sicherheit der Software während des Gebrauchs zu gewährleisten.

	Es liegt in der direkten Verantwortung des Organisation des Gesundheitswesens (Einzelperson, Krankenhaus oder Institution), der das Gerät und die Software verwendet, einen Zeitplan für die ordnungsgemäße Wartung zu erstellen, um Sicherheit und Funktionstüchtigkeit sicherzustellen und das Risiko von Störungen und Gefahrensituationen für Patient und Benutzer zu reduzieren.

	Dieses Gerät und die Software sind für den Einsatz unter der direkten Aufsicht von entsprechend geschultem und autorisiertem medizinischem Personal gedacht.

4.3 Datenschutz

Es werden angemessene Vorkehrungen getroffen, um die Privatsphäre der Nutzer und Patienten zu schützen und sicherzustellen, dass personenbezogene Daten unter Wahrung der Rechte, Grundfreiheiten und der Würde der betroffenen Personen verarbeitet werden, insbesondere in Hinblick auf Vertraulichkeit, persönliche Identität und das Recht auf Schutz personenbezogener Daten.

"Personenbezogene Daten" sind im DSGVO definiert als alle Daten über eine identifizierte oder identifizierbare natürliche Person ("betroffene Person"). Eine identifizierbare natürliche Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Bezugnahme auf einen Identifikator wie einen Namen, eine Identifikationsnummer, Ortsdaten, einen Online-Identifikator oder einen oder mehrere Faktoren, die für die physische, physiologische, genetische, geistige, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person spezifisch sind.

Besondere Aufmerksamkeit gilt den Daten, die in der "Allgemeinen EU-Datenschutzverordnung 2016/679 (GDPR)" als "Kategorien sensibler personenbezogener Daten" definiert sind.

Kategorie sensibler personenbezogener Daten
(...) Personenbezogene Daten, aus denen sich die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder Gewerkschaftszugehörigkeit ableiten lassen sowie genetische Daten, biometrische Daten für den Zweck der eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten natürlicher Personen hinsichtlich deren Sexualleben oder sexuellen Orientierung;

Die Gesundheitsorganisation muss sicherstellen, dass die Verwendung des Produkts im Einklang mit den Anforderungen der anwendbaren Vorschriften zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten steht, insbesondere im Hinblick auf die Verwaltung der oben genannten Informationen.

Digistat® verwaltet die folgenden personenbezogenen Daten:

- Vor- und Nachnahme
- Geburtsdatum
- Geschlecht
- Patientencode
- Aufnahmedatum
- Entlassungsdatum
- Körpergewicht
- Körpergröße

Das Produkt kann so konfiguriert werden, dass diese Daten auf jedem Anwendungsbildschirm automatisch ausgeblendet werden.
Stellen Sie dazu in der Produkt-Konfigurationsanwendung die Systemoption "Privacy Mode" auf "true" (siehe Konfigurations- und Installationshandbuch von Digistat). Der Standardwert ist "true".
Wenn die Option "Privacy Mode" auf "true" gesetzt ist, sind folgende Fälle möglich:

- Wenn kein Benutzer angemeldet ist, werden keine Patienteninformationen angezeigt.

- Wenn ein Benutzer angemeldet ist und der Benutzer keine spezielle Berechtigung hat, werden keine Patienteninformationen angezeigt.
- Wenn ein Benutzer angemeldet ist und der Benutzer eine bestimmte Berechtigung hat, werden Patienteninformationen angezeigt.

Die Option kann auf einen einzelnen Arbeitsplatz angewendet werden (d. h. verschiedene Arbeitsplätze können unterschiedlich konfiguriert werden).

Die in diesem Abschnitt aufgeführten Vorkehrungen müssen gelesen und strikt eingehalten werden.

- Die eingesetzten PCs dürfen bei offenen Sessions des Produkt nicht unbeaufsichtigt bleiben und daher für andere Personen zugänglich sein. Es wird dringend empfohlen, sich bei jedem Verlassen des Arbeitsplatzes vom Produkt abzumelden.
- Die in das Produkt eingegebenen personenbezogene daten wie Passwörter oder Personaldaten der Benutzer und Patienten müssen durch geeignete Software (Antivirus, Firewall) vor jedem Versuch unbefugten Zugriffs geschützt werden. Die Implementierung dieser Software ist Aufgabe des Krankenhauses. Diese Software muss in regelmäßigen Abständen aktualisiert werden.

Personenbezogene Daten können in einigen von Produkt erstellten Berichten enthalten sein. Die Gesundheitsorganisation muss diese Dokumente in Übereinstimmung mit den aktuellen Standards zum Schutz der Privatsphäre und der personenbezogenen Daten verwalten.

Client-Workstations (sowohl Desktop als auch Mobile) speichern keine Patientendaten auf der Festplatte. Patientendaten werden nur in der Datenbank gespeichert und der Datenbankspeicher hängt von den Prozeduren und Auswahlmöglichkeiten der Gesundheitsstruktur ab (Beispiele: physische Maschine, SAN, Virtualisierungsumgebung). Patientendaten werden gemäß allen aktuellen Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten behandelt.

Patientendaten werden nicht in proprietären Dateien gespeichert. Der einzige Ort, an dem Patientendaten gespeichert werden, ist die Datenbank.

Unter bestimmten Umständen werden Personal- und/oder empfindliche Daten unverschlüsselt und unter Nutzung einer nicht eigensicheren Verbindung gesendet. Ein Beispiel dafür sind HL7-Mitteilungen. Es ist Aufgabe der verantwortlichen Organisation,

	innerhalb des krankenhausinternen Netzes angemessene Sicherheitseinrichtungen vorzusehen, um die Einhaltung der Gesetze und Vorschriften bezüglich des Datenschutzes zu gewährleisten.
	Es wird empfohlen, den Datenbankserver so zu konfigurieren, dass die Produkt-Datenbank auf der Festplatte verschlüsselt ist. Um diese Option zu aktivieren, wird SQL Server Enterprise Edition benötigt. Während der Installation muss die Option TDE (Transparent Data Encryption) aktiviert sein.
	Die Gesundheitsorganisation hat die Aufgabe, eine Grundausbildung in Fragen des Datenschutzes anzubieten: dies umfasst die Grundprinzipien, Regeln, Vorschriften, Verantwortlichkeiten und Sanktionen in der jeweiligen Arbeitsumgebung. Ascom UMS/Distributor bietet spezielle Schulungen zur optimalen Nutzung des Produkts in Bezug auf Datenschutzfragen an (z. B. Anonymisierung der Datenbank, Datenschutzmodus, Benutzerberechtigungen usw.).
	Die Gesundheitsorganisation muss die folgenden Unterlagen erstellen und aufbewahren: 1) Die aktualisierte Liste der Systemadministratoren und des Wartungspersonals; 2) Die unterzeichneten Auftragsformulare und die Bescheinigungen über die Teilnahme an den Schulungen; 3) Ein Verzeichnis der Anmeldedaten, Berechtigungen und Privilegien, die den Benutzern gewährt werden; 4) Eine aktualisierte Liste der Benutzer des Produkts.
	Die Gesundheitsorganisation muss ein Verfahren zur automatischen Deaktivierung nicht mehr aktiver Benutzer nach einem bestimmten Zeitraum einführen, testen und zertifizieren.
	Die Gesundheitsorganisation muss ein Verfahren zur regelmäßigen Überprüfung der Zugehörigkeit zur Rolle des Systemadministrators und des technischen Wartungspersonals kodifizieren, umsetzen und dokumentieren.

	Die Gesundheitsorganisation führt Prüfungen und Kontrollen des korrekten Verhaltens der Betreiber durch.

	Datenbanken, die Patientendaten/sensible Informationen über dieselben enthalten, dürfen das Gesundheitszentrum nicht ohne vorherige Verschlüsselung/Verschleierung verlassen.

4.3.1 Merkmale und Verwendung der Anmeldeinformationen des Benutzers

Dieser Abschnitt liefert Angaben über die Merkmale, die die Anmeldeinformationen für den Zugriff auf Produkt (Benutzername und Passwort) aufweisen müssen, sowie über deren Verwendung und Beibehaltung.

- Alle Benutzer müssen jede mögliche Vorsichtsmaßnahme ergreifen, um den eigenen Benutzernamen und das eigene Password geheim zu halten.

- Benutzername und Passwort sind privat und persönlich. Der eigene Benutzername und das Passwort dürfen keinesfalls anderen Personen mitgeteilt werden.

- Jeder Benutzer kann eine oder auch mehrere Anmeldeinformationen für die Authentifizierung besitzen (Benutzername und Passwort). Der gleiche Benutzername und das gleiche Passwort dürfen nicht mehreren Benutzern zugeteilt werden.

- Die Anmeldeprofile müssen mindestens einmal jährlich kontrolliert und erneuert werden.

- Es ist möglich, für gleiche Aufgabenbereiche verschiedene Anmeldeprofile der Benutzer zu gruppieren.

- Bei der Definition der Benutzer-Accounts empfiehlt es sich, immer eine namentliche Identifizierung vorzunehmen, anstatt allgemeingültige Benutzer festzulegen wie beispielsweise “ADMIN” oder “PFLEGER”. Jeder Account darf nur für einen einzelnen Benutzer zugänglich sein.

- Jeder Benutzer ist durch ein Profil gekennzeichnet, das ihm den Zugriff nur auf diejenigen Funktionen des Systems gestattet, die zu seinem Aufgabenbereich gehören. Der Systemadministrator muss beim Anlegen des Benutzer-Accounts das entsprechende Profil zuordnen. Dieses Profil muss mindestens einmal pro Jahr revidiert werden. Eine solche Revision kann auch nach Benutzerklassen erfolgen. Die Abläufe zur Festlegung des Benutzerprofils sind im Konfigurations-Handbuch des Produkts beschrieben.

- Das Passwort muss aus mindestens acht Zeichen bestehen.

- Das Passwort darf keine Angaben enthalten, die unmittelbar auf den Benutzer schließen lassen (z.B. Vor- oder Nachname, Geburtsdatum usw.).

- Das Passwort wird vom Systemadministrator zugewiesen und muss vom Benutzer anlässlich der ersten Anmeldung am System geändert werden.

- Danach muss das Passwort mindestens alle drei Monate geändert werden.

- Wenn die Zugriffsinformationen (Benutzername und Passwort) mehr als sechs Monate lang nicht verwendet werden, müssen sie ungültig gemacht werden. Von dieser Regel ausgenommen sind spezifische Zugriffsinformationen, die für technische Wartungszwecke dienen. Die Abläufe zur Konfiguration dieses besonderen Merkmals sind im technischen Handbuch des Produkt beschrieben.

- Die Anmeldeinformationen müssen auch dann ungültig gemacht werden, wenn dem Benutzer die Qualifikation entzogen wird, die diesen Anmeldeinformationen entspricht (z.B. wenn ein Benutzer in ein anderes Krankenhaus wechselt). Der Systemadministrator kann einen Benutzer von Hand freigeben oder sperren. Die Vorgehensweise dazu ist im Konfigurations-Handbuch des Produkts beschrieben.

Die nachstehenden Informationen sind für die Techniker bestimmt, die als Systemadministratoren fungieren:

Das Passwort muss eine "regular expression" einhalten, die in der Produkt-Konfiguration festgelegt ist (der Default-Wert beträgt ^.....*, d.h. 8 Zeichen).
Das Passwort wird vom Systemadministrator in dem Moment zugewiesen, in dem ein neuer Benutzer-Account angelegt wird. Der Administrator kann den Benutzer zwingen, dieses Passwort zu ändern und es beim ersten Zugriff auf das System durch ein persönliches Passwort zu ersetzen. Das Passwort wird nach Ablauf einer konfigurierbaren Zeit ungültig. Der Benutzer ist gehalten, bei Ablauf dieses Zeitraums sein Passwort zu ändern. Es besteht auch die Möglichkeit, das Ungültig werden des Passworts eines Benutzers zu verhindern.

Detaillierte Informationen über die Festlegung der Benutzer-Accounts und die Konfiguration der Passwörter sind dem Konfigurations-Handbuch des Produkt zu entnehmen.

4.3.2 Systemadministratoren

Bei Ausführung der normalen Arbeiten zur Installation, Aktualisierung und technischen Unterstützung der Produkt - Software kann das Personal der Fa. Ascom UMS bzw. der Vertragshändler auf die in der Datenbank des Produkt gespeicherten persönlichen und empfindlichen Daten zugreifen und diese verarbeiten.

Ascom UMS/die Händler wenden beim Management und der Verarbeitung von persönlichen und empfindlichen Daten Prozeduren und Arbeitsanweisungen an, die mit den Vorschriften der einschlägigen Datenschutzgesetze konform sind (“General Data Protection Regulation - EU 2016/679”).

Zur Ausführung der genannten Vorgänge konfiguriert sich das Personal der Fa. Ascom UMS/der Händler als "Systemadministrator" des Produkt (siehe Maßnahme der ital. Datenschutzbehörde bezüglich "Systemadministratoren" vom 25.11.2008). Das von Ascom UMS/dem Händler mit der Ausführung dieser Tätigkeit betraute Personal wird im Hinblick auf die Datenschutzvorschriften und insbesondere auf die Verarbeitung empfindlicher Daten ausreichend geschult.

Um die Anforderungen der Maßnahme über "Systemadministratoren" zur erfüllen muss die verantwortliche Organisation:

- Die Zugriffsberechtigungen namentlich festlegen;
- Das Log für den Zugriff auf der Ebene des Betriebssystems sowohl auf dem Server als auch auf den Clients aktivieren;
- Das Log für den Zugriff auf den Datenbank-Server Microsoft SQL Server (Audit Level) aktivieren;
- Beide Logs so konfigurieren und verwalten, dass die Zugriffe für einen Zeitraum von mindestens einem Jahr zurückverfolgt werden können.

4.3.3 System-Log

Das Produkt registriert die System-Logs in der Datenbank. Diese Logs bleiben über einen konfigurierbaren Zeitraum hinweg gespeichert. Die Logs werden je nach ihrer Art für unterschiedliche Zeiträume gespeichert. Als Default-Werte sind folgende Zeiträume eingestellt:

- Info-Logs werden 10 Tage lang gespeichert;
- Einer Warnung entsprechende Logs bleiben 20 Tage lang gespeichert;
- Einem Fehler entsprechende Logs bleiben 30 Tage lang gespeichert;

Diese Zeiträume sind jedoch konfigurierbar. Die Vorgehensweise zur Festlegung der Speicherungs-Zeiträume der Logs ist dem Konfigurations-Handbuch zu entnehmen.

4.3.4 Forensisches Protokoll

Eine Teilmenge der vorgenannten Systemprotokolle, die gemäß der Richtlinie jeder spezifischen Struktur des Gesundheitswesens unter Verwendung des Produkts als "klinisch relevant" oder "klinisch nützlich" definiert sind, kann an ein externes System (entweder SQL-Datenbank oder Syslog) gesendet und entsprechend den Anforderungen und Regeln der Struktur des Gesundheitswesens gespeichert werden.

4.4 Backup- Richtlinie

Es wird empfohlen, die Produktdatenbank regelmäßig zu sichern.

Die Organisation des Gesundheitswesens, die das Produkt betreibt, muss die Backup-Richtlinie bestimmen, die am besten den Erfordernissen im Hinblick auf die Sicherheit der Daten entspricht.
Ascom UMS bzw. der Vertragshändler stehen zur Verfügung, um die notwendige Unterstützung zur Implementierung der festgelegten Backup- Richtlinie zu liefern.

Das Organisation des Gesundheitswesens muss sicherstellen, dass die generierten Backup-Dateien so archiviert werden, dass sie bei Bedarf umgehend zur Verfügung stehen.

Sofern die Daten auf mobilen Datenträgern gespeichert werden, muss die Organisation des Gesundheitswesensdiese Datenträger so verwahren, dass ein unbefugter Zugriff verhindert wird. Wenn solche Datenträger nicht mehr benutzt werden, müssen sie vernichtet oder definitiv gelöscht werden.

4.5 Vorgehensweise zur Außerbetriebnahme

Es wird empfohlen, eine Sicherung des Abbilds der Festplatte der Arbeitsplatzrechner durchzuführen, so dass im Falle eines Austauschs der Hardware eine schnelle Wiederherstellung der Betriebsumgebung möglich ist.

Wartungsverfahren und Reparaturen müssen in Übereinstimmung mit den Verfahren und Richtlinien von Ascom UMS (oder ihrem Vertriebspartner) und nur von Ascom UMS (oder seinem Vertriebspartner) oder speziell von Ascom UMS (oder seinem Vertriebspartner) speziell autorisierten und autorisierten Mitarbeitern durchgeführt werden.

Dieser Abschnitt beschreibt die von Ascom UMS empfohlene Vorgehensweise bei einer Störung an einen Produkt-Arbeitsplatz. Ziel des hier beschriebenen Vorgangs ist es, die zum Austausch des defekten Arbeitsplatzes durch einen richtig funktionierenden erforderliche Zeit zu minimieren.

Ascom UMS rät zu diesem Zweck, als Ersatzgerät, einen zusätzlichen PC verfügbar zu halten, auf dem Produkt bereits installiert wurde.

Bei einer Störung an einem Produkt-Arbeitsplatz kann das Ersatzgerät sofort diesen Produkt-Arbeitsplatz ersetzen.

Beachten Sie, dass Produkt ur von geschultem und zugelassenem Personal installiert werden darf. Dazu gehören das Personal von Ascom UMS/Vertriebshändlern und alle anderen speziell geschulten und ausdrücklich vom Ascom UMS/Vertriebshändler Personen. Ohne eine ausdrückliche, direkte Genehmigung vom Ascom

UMS/Vertriebshändler ist das Krankenhauspersonal nicht befugt, die Installationsvorgänge auszuführen und/oder die Konfiguration von Produkt zu ändern.

Die Gefahr bezüglich einer Deaktivierung und einem Austausch des Produkt-Arbeitsplatzes besteht in der Zuordnung eines Arbeitsplatzes zu einem falschen Bett oder Zimmer. Dies kann zu einer "Verwechslung des Patienten" führen, was eine besonders gefährliche Situation ist.

In Bezug auf den Austausch und/oder die Neukonfiguration der bei der Datenerfassung über Produkt mitwirkenden Netzwerkausrüstung (z.B. Port Server, Docking Station, usw. ...) besteht die Gefahr, dass die erfassten Daten dem falschen Patienten zugeordnet werden. Die Beziehung zwischen Patient und erfassten Daten basiert auf der IP-Adresse. Ihre Änderung kann entweder zu einer Unterbrechung des Datenflusses oder, in schweren Fällen, zu einer Zuordnung von Daten zu einem falschen Patienten führen.

Die Außerbetriebnahme und der Austausch eines Arbeitsplatzes sind potentiell gefährlich. Das ist der Grund, weshalb diese Vorgänge nur von befugtem und geschultem Personal ausgeführt werden dürfen.
Die mit diesem Vorgang verbundenen Gefahren sind die einer Zuordnung eines falschen Bettes/Bereichs zum Arbeitsplatz und demzufolge der Anzeige von Daten, die nicht zu den entsprechenden Patienten/Betten gehören.

Muss ein Produkt-Arbeitsplatz ausgeschaltet und ausgetauscht werden, muss das Krankenhauspersonal sofort Ascom UMS (oder einen zugelassenen Vertragshändler) verständigen und um das Ausführen dieses Vorgangs bitten.
Wir raten der Krankenhausverwaltung (oder dem, der dafür zuständig ist), zu diesem Zweck einen klaren, eindeutigen Ablauf festzulegen und diesen allen einbezogenen Personen des Personals bekannt zu geben.

Zur Verkürzung der Zeiten für den Austausch raten wir, ein oder mehrere Ersatzgeräte bereit zu halten, auf denen alle notwendigen Anwendungen (Betriebssystem, Firewall, Antivirus, RDP, ...) und Produkt bereits installiert, aber deaktiviert sind (d.h. nicht von einem Benutzer ohne Unterstützung eines Technikers von Ascom UMS ausführbar).
Bei einer Störung an einem Produkt-Arbeitsplatz gewährleistet die Verfügbarkeit des Ersatzgerätes die Minimierung der Wiederherstellungszeit (Austausch der Hardware) und begrenzt zugleich die Gefahr einer Verwechslung von Patienten.

Bei einer Störung an einem Produkt-Arbeitsplatz raten wir, wenn ein “Ersatzgerät” zur Verfügung steht, den folgenden Ablauf anzuwenden:

1) Das Krankenhauspersonal ersetzt den defekten PC durch das “Ersatzgerät”;
2) Das Krankenhauspersonal verständigt Ascom UMS/Vertriebshändler und bittet um die Aktivierung des “Ersatzgerätes”;
3) Das Personal von Ascom UMS/Vertriebshändler deaktiviert den defekten Arbeitsplatz und konfiguriert das “Ersatzgerät” richtig.
4) Der defekte PC wird repariert und als "Ersatzgerät" vorbereitet.

Die Anleitung zu den Vorgängen des Aktivierens/Deaktivierens und zum Austausch eines Produkt-Arbeitsplatzes, die den Systemverwaltern vorbehalten sind, befinden sich im Produkt-Konfigurationshandbuch.

4.5.1 Neukonfiguration oder austausch eines netzapparats

Wenn ein Netzapparat neu konfiguriert oder ausgetauscht werden soll, der an der Datenerfassung von Produkt beteiligt ist, muss das Krankenhauspersonal rechtzeitig Ascom UMS oder dessen Vertragshändler benachrichtigen, damit deren Personal die Neu-Konfiguration von Produkt vornehmen oder die Informationen liefern kann, die zur Ausführung dieses Vorgangs erforderlich sind. Der verantwortlichen Organisation wird empfohlen, einen eindeutigen internen Ablauf zur Abwicklung einer solchen Anforderung festzulegen, der allen betroffenen Personen bekannt sein muss. Im Konfigurations-Handbuch von Produkt sind die Angaben zur Ausführung des genannten Vorgangs enthalten.

4.6 Vorbeugende Wartung

Wartungsverfahren und Reparaturen müssen in Übereinstimmung mit den Verfahren und Richtlinien von Ascom UMS (oder ihrem Vertriebspartner) und nur von Ascom UMS (oder seinem Vertriebspartner) oder speziell von Ascom UMS (oder seinem Vertriebspartner) speziell autorisierten und autorisierten Mitarbeitern durchgeführt werden.

Die Wartung des Produkts sollte mindestens einmal jährlich vorgenommen werden. Dabei ist jedoch zu berücksichtigen, dass das Wartungsintervall der Komplexität des Systems Rechnung tragen muss. Bei sehr komplexen Systemen sollte die Wartung häufiger, d.h. bis zu zweimal pro Jahr erfolgen.

Die Checkliste für die Wartung finden Sie im Installations- und Konfigurationshandbuch des Produkts.

4.7 Kompatible Geräte

Wenden Sie sich bitte an Ascom UMS/Vertriebshändler, um eine Liste der verfügbaren Treiber zu erhalten.

	Der Produkt ist nicht dazu bestimmt, zu überprüfen, ob die Geräte richtig arbeiten, sondern um klinische Daten zu erfassen und zu katalogisieren
	Das Abtrennen eines Gerätes während des Betriebs verursacht eine Unterbrechung der Datenerfassung auf dem Produkt. Gerätedaten, die während der Abschaltzeit verloren werden, können nach dem erneuten Anschließen von Produkt nicht wiederhergestellt werden.
	Deaktivieren Sie niemals die Alarmmeldung auf den Medizinprodukten, es sei denn, dies ist durch die Dokumentation des Medizinproduktherstellers und das Verfahren der Gesundheitsorganisation ausdrücklich erlaubt.
	Die Richtigkeit der von dem Produkt angezeigten Parameter muss immer auf dem Original-Medizinprodukt überprüft werden, das sie erzeugt hat.
	Nie deaktivieren Sie das Audio auf den Arbeitsstationen, auf denen dem Produkt läuft.
	Aus Gründen, die nicht von der Software abhängig sind (wie zum Beispiel, die Art, wie die technischen Geräte installiert/verkabelt sind), sind Verzögerungen zwischen der Auslösung des Alarms und der eigentlichen Anzeige des Alarms möglich.
	Bei Verwendung des allgemeinen Alaris® Drivers, müssen mindestens zehn Sekunden nach dem Trennen einer Infusionspumpe abgewartet werden, bevor eine andere angeschlossen wird.
	Die durch den Anschluss des Gerätes, die Abschaltung, das Trennen und eine Statusänderung hervorgerufene Aktualisierung der auf dem Bildschirm angezeigten Daten ist von der Zeit abhängig, die das Gerät benötigt, um die Änderungen weiterzuleiten. Diese Zeit ist von verschiedenen Faktoren abhängig. Dazu gehören die Geräte- und die Anschlussart. Bei einigen Geräten liegen Bedingungen vor, unter denen die Verzögerung bei der Weiterleitung der Änderungen wichtig sein kann. Da sie je nach der Konfiguration des Gerätes und den Betriebsbedingungen variieren können, ist es nicht möglich, eine Angabe der Verzögerungen für alle möglichen Geräte zu liefern.

	Die zum Einlesen der Daten von den angeschlossenen medizinischen Geräten verwendeten Treiber haben einen Lese-Zyklus von weniger als 3 Sekunden (d.h. die Daten der Geräte werden maximal alle 3 Sekunden gelesen). Allerdings gibt es Geräte, die die Daten weniger häufig übertragen (Intervall von 5-10 Sekunden). In der spezifischen Dokumentation zum Treiber finden Sie Details zum Lese-Zyklus. In einer Testumgebung, die wie im "Installations- und Konfigurationshandbuch Digistat-Server" beschrieben installiert und konfiguriert ist, dauert es, nachdem ein Treiber einen Alarm erkannt hat, maximal 1 Sekunde, um ihn an die Produkt zu übertragen.

	Bei einem Stromausfall benötigt das Produkt einige Minuten, um wieder vollkommen funktionstüchtig zu sein und löst deshalb Alarmmeldungen aus (gewöhnlich die diese Zeit geringer als 3 Minuten, dies ist jedoch von der Konfiguration der verwendeten Computer abhängig).

4.8 Nichtverfügbarkeit des Produkts

Wenn während der Startphase Probleme bei der Verbindung mit dem Server auftreten, meldet das Produkt dies mit einer entsprechenden Ansicht.

Das Problem der Verbindungsherstellung begibt sich möglicherweise in kurzer Zeit von selbst. Sollte dies nicht der Fall sein, muss der Kundendienst benachrichtigt werden. Siehe dazu die Kontaktliste auf Seite 37.

In seltenen, jedoch durchaus möglichen Extremfällen kann es vorkommen, dass das Produkt nicht benutzt werden kann (z.B. bei Naturkatastrophen, anhaltendem Ausfall des Stromnetzes usw.).

Für derartige Fälle muss das Krankenhaus, das Produkt verwendet, eine Notabwicklung festlegen, die in solchen Fällen eingehalten werden muss. Dadurch soll gewährleistet werden,

1) dass die Stationen ihre Tätigkeit fortsetzen können.
2) Die Verfügbarkeit des Produkts muss so rasch wie möglich wieder hergestellt werden (dazu gehört auch die Frage des Backup-Intervalls, siehe Seite 31).

	Für derartige Fälle muss das Krankenhaus, das Produkt verwendet, eine Notabwicklung festlegen, die im Fall mangelnder Verfügbarkeit des Produkts eingehalten werden muss.

Ascom UMS bzw. der zuständige Vertragshändler stehen zur Verfügung, um volle Unterstützung bei der Festlegung dieser Notabwicklung zu bieten. Kontaktliste siehe Seite 37.

5. Kontakte des Herstellers

Wenden Sie sich für jegliche Fragen zuerst an den Vertriebshändler, der das Produkt installiert hat.
Hier folgend die Kontakte für den Hersteller:

Ascom UMS s.r.l unipersonale

Via Amilcare Ponchielli Nr. 29, 50018, Scandicci (FI), Italien
Tel. (+39) 055 0512161
Fax (+39) 055 8290392

Technischer Kundendienst

support.it@ascom.com
800999715 (gebührenfrei, nur von Italien)

Vertrieb und Produktinformationen

it.sales@ascom.com

Allgemeine Informationen

it.info@ascom.com

6. Restrisiken

Im Lebenszyklus von der Produkt wurde ein Risikomanagementprozess implementiert, der die relevanten technischen Standards übernimmt. Es wurden Maßnahmen zur Risikokontrolle identifiziert und umgesetzt, um Risiken auf ein Minimum zu reduzieren und sie im Vergleich zu den Vorteilen des Produkts akzeptabel zu machen. Das gesamte Restrisiko ist auch im Vergleich zu den gleichen Leistungen akzeptabel.

Die nachfolgend aufgeführten Restrisiken wurden berücksichtigt und auf ein Minimum reduziert. Aufgrund des dem Konzept "Risiko" innewohnenden Charakters ist es nicht möglich, dieses vollständig zu beseitigen; diese Restrisiken sind den Nutzern offen zu legen.

- Die Unfähigkeit, Digistat oder einige seiner Funktionalitäten erwartungsgemäß zu verwenden, kann zu Verzögerungen und/oder Fehlern bei den therapeutischen/diagnostischen Maßnahmen führen.
- Nicht autorisierte Handlungen der Benutzer können Fehler bei den therapeutischen/diagnostischen Maßnahmen und der Zuweisung von Verantwortlichkeiten für diese Handlungen verursachen.
- Zuordnung von Informationen zum falschen Patienten (Patientenaustausch), was zu Verzögerungen und/oder Fehlern bei den therapeutischen/diagnostischen Maßnahmen führen kann.
- Der fehlerhafte Umgang mit Patientendaten, einschließlich Fehlern bei der Anzeige, dem Hinzufügen, der Bearbeitung und dem Löschen von Daten, können zu Verzögerungen und/oder Fehlern bei den therapeutischen/diagnostischen Maßnahmen führen.
- Off-Label-Verwendung von Digistat (z. B. Verwendung des Produkts als primäres Alarmmeldesystem, therapeutische oder diagnostische Entscheidungen und Eingriffe, die ausschließlich auf den vom Produkt bereitgestellten Informationen basieren).
- Unbefugte Offenlegung von personenbezogenen Daten von Benutzern und/oder Patienten.

RISIKEN DER FÜR DAS MEDIZINPRODUKT EINGESETZTEN HARDWARE-PLATTFORM

- Stromschlag bei Patienten und/oder Bediener, was zu Verletzungen oder zum Tod des Patienten und/oder des Bedieners führen kann.
- Überhitzung der Hardware-Komponenten, was zu leichten Verletzungen des Patienten und/oder des Bedieners führen kann.
- Befall des Patienten und/oder des Bedieners durch Infektionen.