Digistat® Docs Benutzerhandbuch

Version 2.0

2020-12-22

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® Docs Version 1.1
Digistat® Docs wird von der Ascom UMS srl hergestellt (http://www.ascom.com).

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
Digistat® Docs darf nur nach Erhalt einer gültigen Lizenz von Ascom UMS oder dem Vertriebspartner verwendet werden.

Lizenzen sind eingetragene warenzeichen
Digistat® ist eine Marke der Ascom UMS s.r.l. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

Diese Veröffentlichung darf ohne die vorherige schriftliche Genehmigung von Ascom UMS weder ganz noch auszugsweise in einer beliebigen Form und mit beliebigen Mitteln vervielfältigt, übermittelt, kopiert, gespeichert oder übersetzt werden.

Inhaltsverzeichnis

1. Verwendung des Handbuchs 5

1.1 Ziele 6

1.2 Verwendete Zeichen und Terminologie 6

1.3 Konventionen 6

1.4 Symbole 7

1.5 Die Digistat Suite Übersicht 8

1.6 Die Info-Anzeige 8

2. Digistat Docs 9

2.1 Bestimmungsgemäße 9

2.2 Zulassungsüberschreitende (Off-label) Anwendung des Produkts 10

2.3 Patientenzahl 10

2.4 Sicherheitshinweise 10

2.5 Restrisiken 12

2.6 Verantwortlichkeiten der Organisation des Gesundheitswesens 13

2.7 Verantwortlichkeit des Herstellers 14

2.8 Rückverfolgbarkeit des Produkts 14

2.9 After-Sales-Aufsichtssystem 14

2.10 Standzeit des Produkts 14

3. Software/Hardware spezifikationen 15

3.1 Bettseitig 16

3.1.1 Hardware 16

3.1.2 Betriebssystem 16

3.1.3 System Software 16

3.2 Server 17

3.2.1 Hardware 17

3.2.2 Betriebssystem 17

3.2.3 System Software 17

3.3 Digistat Mobile 17

3.4 Digistat Gateway 18

3.5 Digistat Web 18

3.6 Allgemeine Warnungen 18

3.7 Audio / Video-Streaming-Funktionalität 19

3.8 Firewall und Antivirus 20

3.8.1 Weitere empfohlene Vorsichtsmaßnahmen für den Cyberschutz 21

3.9 Eigenschaften des lokalen Netzes 22

4. Vor dem Start 23

4.1 Vorschriften für Installation und Wartung 23

4.2 Datenschutz 24
4.2.1 Merkmale und Verwendung der Anmeldeinformationen des Benutzers 27
4.2.2 Systemadministratoren 28
4.2.3 System-Log 29
4.2.4 Forensisches Protokoll 29
4.3 Kompatible Geräte 30
4.4 Nichtverfügbarkeit des Produkts 31
5. Kontakte des Herstellers 32

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 Modulen finden Sie in den entsprechenden Handbüchern:

USR DEU Controlbar Web
USR DEU Codefinder
USR DEU Codefinder Web
USR DEU Diary
USR DEU Forms
USR DEU Forms Web
USR DEU Image Bank
USR DEU Messenger
USR DEU Dashboard
USR DEU On Line
USR DEU Nutrition
USR DEU Stock Management

USR DEU OranJ
USR DEU Smart Scheduler
USR DEU Therapy
USR DEU Voice Notes Mobile
USR DEU Identity Mobile
USR DEU Collect Mobile
USR DEU BCMA (Mobile)
USR DEU Gateway (Mobile)

Dieses Benutzerhandbuch kann auch in Kombination mit den folgenden Dokumenten verwendet werden, da es sich um die zugehörigen Digistat Care-Module handelt, die von Digistat Docs verwendet werden:

USR DEU ControlBar
USR DEU Patient Explorer
USR DEU Mobile Launcher

Weitere Informationen finden Sie in Abschnitt 1.5.

1.1 Ziele

Dieses Handbuch enthält alle notwendigen Informationen für eine sichere und korrekte Anwendung von Digistat Docs und ermöglicht die Identifizierung des Herstellers. Darüber hinaus dient es als Orientierungshilfe für den Benutzer, der wissen möchte, wie bestimmte Operationen durchzuführen sind, sowie als Leitfaden für die korrekte Verwendung der Software, um potenziell gefährlichen Missbrauch zu verhindern.

1.2 Verwendete Zeichen und Terminologie

Die Verwendung von Digistat Docs erfordert Grundkenntnisse der gängigsten IT-Begriffe und -Konzepte. Zum Verständnis dieses Handbuchs sind solche Kenntnisse ebenfalls erforderlich. Die Nutzung von Digistat Docs ist zudem nur fachlich qualifiziertem und autorisiertem, geschultem Personal vorbehalten, mit Ausnahme von Laien ei eingeschränkten Funktionen.

Bei der Konsultation der Online-Version im Gegensatz zur Papierversion funktionieren die Querverweise im Dokument als Hypertext-Links. Dies bedeutet, dass der Leser jedes Mal, wenn er auf den Verweis, auf ein Bild (z. B. „Abb. 2“) oder auf einen Absatz/Abschnitt (z. B. „Absatz 2.2.1“) stößt, auf den Verweis klicken kann, um direkt zu dieser bestimmten Abbildung oder zu einem spezifischen Absatz / Abschnitt zu gelangen.

Die in den Bildern in den Ascom UMS-Handbüchern angezeigten klinischen Daten sind in einer Testumgebung erstellte Beispiele und deren einziger Zweck darin besteht, die Struktur und die Verfahren von dem Produkt zu erläutern. Es handelt sich nicht um tatsächliche Daten, die aus klinischen Eingriffen stammen, und gelten auch nicht als solche.

Teile, die sich auf die Konfiguration von dem Produkt beziehen, werden in den Ascom UMS-Handbüchern auf Englisch vorgestellt. Diese Konfigurationen hängen von den tatsächlichen Abläufen und Namen ab, die von der Organisation des Gesundheitswesens mit dem Produkt übernommen wurden, und sind daher in der von der Organisation des Gesundheitswesens angeforderten Sprache verfügbar.

1.3 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.

1.4 Symbole

In diesem Handbuch werden die folgenden Symbole verwendet.

Nützliche Information

Dieses Symbol erscheint heben zusätzlichen Informationen bezüglich der Eigenschaften und der Verwendung von dem Digistat Docs. 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 dem About-Box verwendet:

Name und Adresse des Herstellers

Achtung, begleitende Unterlagen beachten

Dieses Symbol weist auf die Notwendigkeit hin, dass der Benutzer im Hinblick auf wichtige Informationen zur Sicherheit, wie beispielsweise Warnhinweise und Vorsichtsmaßnahmen, die aus verschiedenen Gründen nicht auf dem medizinischen Gerät selbst angegeben werden können, die Bedienungsanleitung konsultieren muss.

1.5 Die Digistat Suite Übersicht

Die Digistat Suite ist ein modulares PDMS, mit dem Lösungen für Anforderungen im Zusammenhang mit der Verwaltung von Patientendaten erstellt werden sollen. Die verschiedenen Lösungen wurden erstellt, um die notwendigen Module bereitzustellen, die Teil der beiden Produkte der Suite sind:

- Digistat Docs (nicht medizinisches Gerät);
- Digistat Care (Medizinprodukt der Klasse IIb).

Digistat Docs ist eine Software, die Patienteninformationen und patientenbezogene Daten aufzeichnet, überträgt, speichert, organisiert und anzeigt, um Pflegepersonen bei der Erstellung einer elektronischen Patientenakte zu unterstützen.
Digistat Docs ist kein medizinisches Produkt.

Digistat Care ist eine Software, die Patienteninformationen und patientenbezogene Daten, einschließlich Daten und Ereignisse von medizinischen Geräten und Systemen, verwaltet und Informationen zur Unterstützung von Behandlung, Diagnose, Prävention, Überwachung, Vorhersage, Prognose und Abschwächung von Krankheiten bereitstellt.
Digistat Care ist ein Medizinprodukt der Klasse IIb.

Da beide Produkte modular aufgebaut sind, kann die jeweilige Gesundheitseinrichtung je nach Bedarf und Zielsetzung entscheiden, ob alle verfügbaren Module oder nur eine Untergruppe aktiviert werden sollen.

Module können zu unterschiedlichen Zeiten hinzugefügt werden. Die resultierende Software-Suite kann sich im Laufe der Zeit entsprechend den möglichen Veränderungen der Anforderungen der Einrichtung ändern. In diesen Fällen werden spezielle zusätzliche Schulungen angeboten und die Konfiguration wird unter Einbeziehung der zuständigen Einrichtung erneut validiert.

1.6 Die Info-Anzeige

Die Schaltfläche **Info** im Digistat Suite-Hauptmenü zeigt ein Fenster mit Informationen zur Digistat-Version und zum installierten Produkt sowie den zugehörigen Lizenzen angezeigt.

Die eigentliche Kennzeichnung steht in der Info-Anzeige, die auf den Client-Arbeitsstationen und Mobilgeräten angezeigt wird, auf denen die Digistat Suite installiert ist.

In Übereinstimmung mit der EU-Verordnung Nr. 207/2012 vom 9. März 2012 wird die Gebrauchsanweisung in elektronischer Form bereitgestellt. Das Info-Feld des Produkts enthält die Adresse einer Webressource, über die die neueste Version der Gebrauchsanweisung heruntergeladen werden kann.

2. Digistat Docs

Digistat Docs erfasst, überträgt, speichert, organisiert und zeigt Patienteninformationen und patientenbezogene Daten, einschließlich Daten von externen Systemen sowie manuell eingegebene Informationen, an, um:

- eine elektronischen Dokumentation der Abteilungsaktivitäten bereitzustellen;
- Informationen zur Verwendung von Materialien und Personal bereitzustellen;
- verschobene Statistiken für die Qualitätskontrolle zu erstellen;
- Remote-Nutzern einige Informationen für nicht-klinische Zwecke anzuzeigen.

Digistat Docs funktioniert zusammen mit Digistat Care, dem anderen Produkt der Digistat Suite. Weitere Informationen finden Sie im Dokument *USR DEU Digistat Care*.

2.1 Bestimmungsgemäße

Digistat Docs ist eine Software, die Patienteninformationen und patientenbezogene Daten aufzeichnet, überträgt, speichert, organisiert und anzeigt, um Pflegepersonen bei der Erstellung einer elektronischen Patientenakte zu unterstützen.

Digistat Docs umfasst:

- Konfigurierbare elektronische Patientenakten, die auf den aufgezeichneten Informationen sowie auf manueller und automatisierter Dokumentation der Aktivität der klinischen Stationen beruhen.
- Speicherung der Ergebnisse und Daten in einem zentralen Daten-Repository.
- Umwandlung der verfügbaren Informationen nach vordefinierten Regeln.
- Datenübertragung von und zu klinischen und nichtklinischen Systemen.
- Planung und Dokumentation der Abteilungsaktivitäten.
- Retrospektive Visualisierung von Daten und Ereignissen.
- Erfassung, Validierung und Anzeige von Vitalzeichen-Diagrammen.
- Konfigurierbare Berichte, Diagramme und Statistiken zur Dokumentation der Patientenakten und zur Analyse der Effizienz, Produktivität, Kapazität und Ressourcenauslastung der Station sowie der Qualität der Versorgung.
- Spezifische Funktionen und Schnittstellen für Laien an entfernten Standorten zur Anzeige von Informationen, Berichten, Diagrammen und Statistiken.

Digistat Docs ist nicht als Entscheidungshilfe für klinische Maßnahmen oder zur direkten Diagnose oder Überwachung wichtiger physiologischer Parameter gedacht.
Die eigenständige Software von Digistat Docs wird auf einer bestimmten Hardware installiert und setzt die ordnungsgemäße Verwendung und den Betrieb der angeschlossenen medizinischen Geräte, Systeme, Anzeigegeräte und des medizinischen Computernetzwerks voraus.
Digistat Docs arbeitet mit Digistat Care, dem anderen Produkt der Digistat Suite, zusammen.
Digistat Docs wird in Gesundheitseinrichtungen auf Intensivstationen, Teilintensivstationen, normalen Stationen und in anderen Abteilungen eingesetzt.
Die Patientengruppe und die Patientenbedingungen werden durch angeschlossene Systeme und durch die spezielle Konfiguration von der Produkt festgelegt, die von der Organisation des Gesundheitswesens angefordert werden.
Die Benutzer sind geschultes medizinisches Fachpersonal mit Ausnahme von Laien ei eingeschränkten Funktionen.

2.2 Zulassungsüberschreitende (Off-label) Anwendung des Produkts

Jede Anwendung des Digistat Docs (das Produkt im Folgenden) 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.

2.3 Patientenzahl

Das Produkt ist für den Einsatz in Verbindung mit medizinischen Geräten und Systemen vorgesehen und bestimmt die Patientenzahl. Das Produkt hat die folgenden technischen Grenzen:

- Gewicht des Patienten zwischen 0,1 kg und 250 kg
- Größe des Patienten zwischen 15 cm und 250 cm

2.4 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.

Zur Verwendung des Produkts in einer klinischen Umgebung müssen alle Komponenten des Systems, zu dem das Produkt gehört, alle geltenden gesetzlichen Anforderungen erfüllen.
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.

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, mit Ausnahme von Laien ei eingeschränkten Funktionen.

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 und andere Störungen 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 und Web Browser.

2.5 Restrisiken

Im Lebenszyklus von dem 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, das Produkt oder einige seiner Funktionalitäten erwartungsgemäß zu verwenden, kann zu Verzögerungen und/oder Fehlern bei den Dokumentationsaktivitäten führen.
- Verlangsamung der Geräteleistung, die zu Verzögerungen und/oder Fehlern bei den Dokumentationsaktivitäten führen kann.
- Nicht autorisierte Handlungen der Benutzer können Fehler bei den Dokumentationsaktivitäten und der Zuweisung von Verantwortlichkeiten für diese Handlungen verursachen.
- Falsche oder unvollständige Konfiguration des Produkts, die zu Verzögerungen und/oder Fehlern bei den Dokumentationsaktivitäten führen kann.
- Zuordnung von Informationen zum falschen Patienten (Patientenaustausch), was zu Verzögerungen und/oder Fehlern bei den Dokumentationsaktivitäten 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 Dokumentationsaktivitäten führen.
- Off-Label-Verwendung des Gerätes (z. B. Produkt, das als primäre Unterstützung für therapeutische oder diagnostische Entscheidungen und Interventionen verwendet wird).
- 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.

2.6 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 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 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
- 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

2.7 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.

2.8 Rückverfolgbarkeit des Produkts

Um die Rückverfolgbarkeit der Geräte zu gewährleisten und Korrekturmaßnahmen vor Ort durchzuführen, muss der Eigentümer 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).
Bei Zweifeln/Fragen zur Produktidentifikation wenden Sie sich bitte an den technischen Kundendienst von Ascom UMS/des Vertriebspartners (Ansprechpartner siehe Absatz 5).

2.9 After-Sales-Aufsichtssystem

Das Produkt 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.
Bei Erhalt einer Rückmeldung von einem Benutzer oder einer internen Benachrichtigung startet Ascom UMS/der Händler unverzüglich die Überprüfung und Verifizierungsprozess starten und die erforderlichen Korrekturmaßnahmen durchführen.

2.10 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

Das Produkt 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 Produkt-Konfiguration zu ändern.

Das Produkt darf nur von geschultem Personal verwendet werden, mit Ausnahme von Laien ei eingeschränkten Funktionen. Das Produkt 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“).
Die Einrichtung des Gesundheitswesens ist dafür verantwortlich, die Umgebung für den Betrieb der Geräte, einschl. Hardware und Software wie in diesem Kapitel beschrieben aufrechtzuerhalten. Die Wartung umfasst Upgrades, Updates und Sicherheitspatches von Betriebssystemen, Webbrowsern und Microsoft.NET Framework, Adobe Reader usw. sowie die Übernahme der anderen bewährten Verfahren für die Wartung von Soft- und Hardwarekomponenten.

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: 22-Zoll-Display, Mindestauflösung 1920x1080, mit integriertem Lautsprecher. Touchscreen empfohlen.
- Maus oder kompatibles Gerät. Touchscreen empfohlen.
- Ethernet- Schnittstelle 100 Mb/s (oder höher)

Für den Fall, dass eine Zentrale oder eine Workstation am Krankenbett für die Anzeige von Videostreams konfiguriert ist (Funktion wird nur in 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: 22-Zoll-Display, Mindestauflösung 1920x1080, mit integriertem Lautsprecher. Touchscreen empfohlen.
- Maus oder anderes kompatibles Gerät. Touchscreen empfohlen.
- Ethernet-Schnittstelle 100 Mb / s (oder höher)

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 8.1 x86/x64 Professional
- Microsoft Corporation Windows 10

3.1.3 System Software

- Microsoft Framework .NET 4.5
- Adobe Acrobat Reader 10

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.

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.

3.2.2 Betriebssystem

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016
- Microsoft Corporation Windows Server 2019

3.2.3 System Software

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Framework.NET 4.5

3.3 Digistat Mobile

Digistat Mobile ist mit Android-Geräten ab Version 4.4.2 bis 10.0 kompatibel. Es wurde auf den Ascom Myco SH1- und SH2-WLAN- und Mobiltelefongeräten mit Android-Version 5.1 (Myco 2) und Android-Version 9.0 (Myco 3) überprüft. Darüber hinaus wurde eine Verifizierung auf dem Gerät Zebra Phone TC51 mit Android Version 7.1 durchgeführt.

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 Gateway

Digistat Gateway ist mit Android-Geräten ab Version 8.0 bis 10.0 kompatibel. Es wurde auf Ascom Myco SH2 Wi-Fi/Cellular (Android 9), Google Pixel 3a (Android 9 und 10), Samsung A10 (Android 9 und 10), Samsung A50 (Android 9 und 10) verifiziert. Die Anwendung wurde dahingehend entwickelt, dass sie mit anderen Android-Geräten mit mindestens einem 5-Zoll-Display kompatibel ist, und die Kompatibilität mit einem bestimmten Gerät muss vor der klinischen Verwendung verifiziert werden.
Um auf alle Funktionalitäten von Digistat Gateway zugreifen zu können, wird eine SIM-Karte mit Sprachplan benötigt. Im Falle einer Installation ohne Wi-Fi-Verbindung wird für den Zugriff auf den Gateway-Treiber auch ein Datenplan benötigt (LTE-Anbindung wird dringend empfohlen).
Bitte wenden Sie sich für die komplette Liste der Geräte, die Digistat Gateway unterstützen, an Ascom UMS/den Lieferanten.

3.5 Digistat Web

Die folgenden Browser werden für die Verwendung mit DIGISTAT®-Web (im Folgenden Digistat Web) Anwendungen unterstützt:

- Chrome 83
- Firefox 77
- Edge 83
- Internet Explorer 11

Die Anzeige-Skalierung des Browsers muss immer auf 100% eingestellt sein.

3.6 Allgemeine Warnungen

Bei mobilen und Desktop-Modulen hängen das Dezimaltrennzeichen und allgemein die vom Produkt verwendeten regionalen Einstellungen (z. B. Datumsformate) von den Einstellungen des Betriebssystems des Arbeitsplatzes oder des mobilen Geräts ab, auf dem das Produkt installiert ist.
Bei Webmodulen hängen das Dezimaltrennzeichen und allgemein die vom Produkt verwendeten regionalen Einstellungen (z. B. Datumsformate) von der Produktkonfiguration ab.

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.

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.

Das Produkt wurde während der Installations- oder Upgrade-Phase verifiziert und validiert, und der Abnahmetest wurde auf der Hardware (PC, Server, mobile Geräte) und Software (z. B. Betriebssystem) zusammen mit anderen bereits vorhandenen Softwarekomponenten (z. B. Browser, Antivirus usw.) durchgeführt. Jede andere installierte Hardware oder Software kann die Sicherheit, Wirksamkeit und Design Controls des Produkts beeinträchtigen.

Bevor andere als die in der Installations- oder Upgrade-Phase validierte Software zusammen mit dem Produkt verwendet wird, ist es zwingend erforderlich, einen autorisierten Ascom UMS/Vertriebspartner zu konsultieren.

Wenn eine andere Software (Dienstprogramme oder Anwendungsprogramme) auf der Hardware, auf der das Produkt läuft, installiert werden muss, muss die Gesundheitseinrichtung Ascom UMS/Distributor zur weiteren Validierung informieren. Es empfiehlt sich, eine Genehmigungsrichtlinie einzuführen, die verhindert, dass Benutzer Verfahren wie die Installation neuer Software durchführen können.

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.

Hardware- und Softwareanforderungen für Geräte von Drittanbietern (einschließlich Smart Adapter Module von Project Engineering, Port Server von Lantronix usw.) werden in den von den Lieferanten bereitgestellten Gebrauchsanweisungen angegeben. Von Ascom oder autorisierten Händlern können Kontaktdatem von Lieferanten der Geräte von Drittanbietern bereitgestellt werden.

3.7 Audio / Video-Streaming-Funktionalität

In bestimmten Konfigurationen implementiert das Produkt Audio- / Video-Streaming-Funktionen.

In den Fällen, in denen 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.

In den Fällen, in denen 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.

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.

3.8 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 Docs 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.

3.8.1 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.

3.9 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.

Wenn das lokale Netzwerk zumindest teilweise auf WLAN-Verbindungen basiert, sind angesichts der möglichen Unterbrechung der WLAN-Verbindung Netzwerkunterbrechungen möglich, die zur Aktivierung des „Wiederherstellungs- oder Unterbrechungsmodus“ (“Recovery or Disconnection Mode”) führen, der, falls das Produkt für die primäre Benachrichtigung über Alarme verwendet wird, die Nichtverfügbarkeit des Systems verursachen kann. Die verantwortliche Organisation sorgt für eine optimale Netzabdeckung und -stabilität und schult die Benutzer in der Verwaltung dieser vorübergehenden Unterbrechungen.

Weitere Informationen zu den erforderlichen Funktionen des lokalen Netzwerks (einschließlich des drahtlosen Netzwerks), in dem die Digistat Suite installiert ist, finden Sie im *Installationshandbuch* und *Konfigurationshandbuch* der Digistat Suite.

---

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.

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.

- Verwenden Sie Geräte von Drittanbietern, die von Ascom UMS /Distributoren empfohlen werden.
- Nur geschulte und autorisierte Personen dürfen Geräte von Drittanbietern installieren.
- 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 Installieren und Wartung zu erstellen, um Sicherheit und Funktionstüchtigkeit sicherzustellen und das Risiko von Störungen und Gefahrensituationen für Patient und Benutzer zu reduzieren.
- Der Speicher-Dongle von dem Produkt (USB-Dongle) wenn verwendet muss unter geeigneten Umgebungsbedingungen (Temperatur, Feuchtigkeit, elektromagnetische Felder usw.) verwahrt und verwendet werden, wie vom Hersteller angegeben. Die Umgebungsbedingungen sind im Wesentlichen die gleichen, die allgemein für elektronische Bürogeräte gefordert 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.
- Die Organisation des Gesundheitswesens muss alternative Arbeitsverfahren definieren, falls das System nicht mehr funktioniert.

4.2 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.
Das Produkt verwaltet die personenbezogenen Daten.
Das Produkt kann so konfiguriert werden, dass es automatisch in den Anwendungsbildschirmen ausgeblendet wird, wenn kein Benutzer in der Teilmenge der persönlichen Daten angemeldet ist, mit denen eine natürliche Person identifiziert werden kann.
Die ausgeblendeten Felder sind:

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

Die ausgeblendeten Felder können während der Konfiguration des Produkts angepasst werden.
Stellen Sie dazu in der Produkt-Konfigurationsanwendung die Systemoption "Privacy Mode" auf "true" (siehe Konfigurations- und Installationshandbuch von dem Produkt). 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.
- Von einer häufigen Verwendung der Sperrfunktion ist unbedingt abzuraten. Das automatische Ausloggen soll dazu beitragen, dass für Unbefugte weniger Möglichkeiten bestehen, auf das Produkt zuzugreifen.
- 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.
- 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.

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.

4.2.1 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 Digistat Installation- und Konfiguration Handbuch 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.3 Kompatible Geräte

Um die vollständige Liste der verfügbaren Geräte zu erhalten, beziehen Sie auf Ascom UMS /Verteiler.

Das Produkt empfängt Daten aus verschiedenen Quellen: medizinische Geräte, Krankenhausinformationssysteme und manuelle Eingaben des Benutzers.
Zusätzlich berechnet das Produkt abgeleitete Informationen (z. B. Scoring).
Der Umfang, die Präzision und die Genauigkeit dieser Daten hängen von den externen Quellen, den vom Benutzer eingegebenen Daten und der zugrunde liegenden Hardware- und Softwarearchitektur ab.

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.

Die Richtigkeit der von dem Produkt angezeigten Parameter muss immer auf dem Original-Medizinprodukt überprüft werden, das sie erzeugt hat.

Die Aktualisierung der auf dem Bildschirm angezeigten Daten, die durch die Verbindung des Geräts, das Ausschalten, das Trennen der Verbindung und die Änderung des Status verursacht wird, hängt von der Zeit ab, die das Gerät selbst benötigt, um die Änderungen zu übermitteln. Diese Zeit ist von verschiedenen Faktoren abhängig. Dazu gehören der Gerätetyp und die Art der Verbindung. 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 Treiber, mit denen die Daten von den angeschlossenen Medizinprodukten gelesen werden, haben einen Lesezyklus 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.

Bei einem Stromausfall benötigt das Produkt einige Minuten, um wieder vollkommen funktionstüchtig zu sein und löst deshalb Daten anzeigen aus.

4.4 Nichtverfügbarkeit des Produkts

Falls die Workstation (einschließlich mobiler Geräte), auf der das Produkt installiert ist, bei der Verbindung mit dem Server auf Probleme stößt, wird eine spezielle Informationsmeldung angezeigt.

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.

Das Produkt versucht, sich automatisch wiederherzustellen. Wenn die automatische Wiederherstellung fehlschlägt, müssen Sie sich an den technischen Support wenden. Siehe dazu die Kontaktliste auf Absatz 5.

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

Ascom UMS bzw. der zuständige Vertragshändler stehen zur Verfügung, um volle Unterstützung bei der Festlegung dieser Notabwicklung zu bieten. Kontaktliste siehe Absatz 5.

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