



Digistat® Produkt Användarmanual

Revision 1.0

2019-06-11

ASCOM UMS s.r.l. Unipersonale

Via Amilcare Ponchielli 29, IT-50018 Scandicci (FI), Italien

Tfn (+39) 055 0512161 – Fax (+39) 055 829030

www.ascom.com

Digistat® version 6.0

Digistat® tillverkas av Ascom UMS s.r.l. (<http://www.ascom.com>).

Produkten Digistat® är  märkt enligt direktiv 93/42/EEG (medicintekniska produkter) ändrat genom direktiv 2007/47/EG.

Ascom UMS är certifierat enligt standarder EN ISO 13485:2016 för “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”.

Programvarulicens

Produkten måste endast användas efter att ha erhållit en giltig licens från Ascom UMS eller Distributören.

Licenser och registrerade varumärken

Digistat® är ett varumärke för Ascom UMS s.r.l. Alla övriga varumärken tillhör respektive ägare.

Ingen del av detta dokument får reproduceras, överföras, kopieras, spelas in eller översättas, i någon form, på något sätt, på något media utan skriftligt förhandstillstånd från Ascom UMS.

Innehåll

1. Att använda manualen	5
1.1 Syfte	5
1.2 Använda tecken och terminologi	5
1.3 Symboler	6
1.3.1 Digistat Om Box	7
2. Introduktion till DIGISTAT	8
2.1 Modulär arkitektur	8
2.2 Avsedd användning	8
2.2.1 Säkerhetsbestämmelser	10
2.3 Användning "off-label" av produkt	11
2.4 Patientbefolkning	11
2.5 Healthcare organization responsibilities	Error! Bookmark not defined.
2.6 Tillverkarens ansvar	12
2.7 Produktens spårbarhet	13
2.8 Uppföljningssystem efter försäljning	13
2.9 Produktens livslängd	13
3. Mjuk- och hårdvarudata	14
3.1 Patientnära	14
3.1.1 Hårdvara	14
3.1.2 Operativsystem	15
3.1.3 Systemmjukvara	15
3.2 Server	15
3.2.1 Hårdvara	15

3.2.2 Operativsystem.....	16
3.2.3 Systemmjukvara	16
3.3 DIGISTAT “Mobile”	17
3.4 DIGISTAT “Web”	17
3.5 Varningar	18
3.6 Brandvägg och virusskydd	19
3.6.1 Ytterligare rekommenderade försiktighetsåtgärder för cyberskydd	20
3.7 Det lokala nätverkets egenskaper	21
3.7.1 DIGISTAT systemets inverkan på vårdenhetsens nätverk.....	22
4. Före användning	23
4.1 Varningsföreskrifter för installation och underhåll	23
4.2 Försiktighetsåtgärder och varningsföreskrifter	24
4.3 Integritetspolicy.....	25
4.3.1 Användning av användarens inloggningsuppgifter och dess egenskaper.....	28
4.3.2 Systemadministratörer	29
4.3.3 Systemloggar.....	30
4.3.4 Forensisk logg.....	30
4.4 Säkerhetskopieringspolicy.....	31
4.5 Procedur vid funktionsfel	31
4.5.1 Omkonfiguration eller utbyte av apparat i nätverket	32
4.6 Förebyggande underhåll.....	34
4.7 Kompatibla enheter.....	34
4.8 Otillgängligt system	36
5. Tillverkarens kontaktuppgifter	37
6. Kvarstående risker	38

1. Att använda manualen

Denna användarmanual ska användas i kombination med modulspecifika manualer, listade nedan. Se tillämpliga manualer, enligt Digistat-modulerna som används i hälsovårdsorganisationen:



USR SWE Smart Central
USR SWE Smart Central Mobile
USR SWE Vitals Mobile
USR SWE Voice Notes Mobile
USR SWE Identity Mobile
USR SWE Collect Mobile

1.1 Syfte

Arbetet med att ta fram denna manual syftar till att erbjuda all nödvändig information för att säkerställa en säker och korrekt användning av Digistat-systemet samt möjligheten att identifiera tillverkaren. Vidare har detta dokument till syfte att beskriva varje enskild del av systemet. Dokumentet är även en referensguide till användaren som vill veta hur ett specifikt moment ska utföras och en guide för korrekt användning av systemet. Detta för att undvika felaktig och potentiellt farlig användning.

1.2 Använda tecken och terminologi

Användningen av Digistat-systemen kräver grundläggande kunskap om de vanligaste IT-termerna och -begreppen. På samma sätt är förståelsen av denna manual föremål för sådan kunskap.

Tänk på att Digistat-systemen endast får användas av professionellt kvalificerad och korrekt utbildad personal.

När online-versionen konsulteras i motsats till pappersversionen, fungerar korsreferenserna i dokumentet som hypertextuella länkar. Detta betyder att varje gång du stöter på referensen till en figur (till exempel Fig. 9) eller ett avsnitt (till exempel avsnitt 4.4) kan du klicka på referensen så att du direkt kommer till den specifika figuren eller det specifika avsnittet.

1.2.1 Textkonvention

Följande begrepp används i detta dokument:

- Benämning på knappar, menykommandon, alternativ, ikoner, fält och allt i användargränssnittet som användaren kan interagera med (antingen tryck eller

klicka eller välj) är formaterade med **fetstil**.

- Benämning / rubriker på skärmar, fönster och flikar är citerade med "Dubbla citationstecken".
- Programmeringskod är formaterad i Courier.
- Punkten ➤ anger en åtgärd som användaren måste utföra för att utföra en specifik åtgärd.
- Referenser till externa dokument är formaterade *kursivt*.

1.3 Symboler

Följande symboler används i denna manual.

Användbar information



Symbolen visas tillsammans med tilläggsinformationen gällande egenskaperna hos och användningen av Digistat. Det kan handla om förklarande exempel, alternativa moment eller extra information som kan vara användbar för att bättre förstå produkten.

Viktigt!



Symbolen lyfter fram information i syfte att förebygga felaktig användning av programvaran eller uppmärksamma kritiska procedurer som kan orsaka risker. Följaktligen är det nödvändigt att vara mycket uppmärksam varje gång som symbolen visas.

Följande symboler används i informationsfältet Digistat (Fig. 1):



Tillverkarens namn och adress



Observera, se bifogad dokumentation

1.3.1 Digistat Om-ruta

Knappen Om på Digistats huvudmeny visar ett fönster som innehåller information om den installerade versionen av Digistat och de relaterade licenserna (Fig. 1). Se användarmanualen för Kontrollpanelen för mer information.



Fig. 1

2. Introduktion till Digistat

Programsviten hos Digistat kliniska moduler är ett avancerat programvarusystem för hantering av patientdata som är specifikt utformat för att användas av läkare, sjuksköterskor och administratörer.

Programvarupaketet innefattar en uppsättning av moduler som antingen kan arbeta enskilt eller vara helt integrerade för att ge en komplett lösning för hantering av patientdata.

Digistat kan användas i flera olika miljöer, allt från intensivvårdsenheter till avdelningar och operationssalar till administrationsavdelningar.

Den modulära arkitekturen och de omfattande konfigurationsmöjligheterna hos Digistat gör att du kan bygga ditt eget system för hantering av patientdata och expandera systemet så att det uppfyller dina nya krav när det behövs.

Det går endast att få åtkomst till Digistat systemet med användarnamn och lösenord. Varje användare definieras av en detaljerad profil och användaren får endast åtkomst till tillåtna områden. Systemet genererar automatiskt en redovisningsspårning över alla utförda inloggningar.

2.1 Modulär arkitektur

Modulär arkitektur betyder att olika produkter (eller moduler) kan implementeras inom samma programvarumiljö (Digistat i detta fall) som karakteriseras av ett konsekvent användargränssnitt, samma allmänna mål och användningsvillkor.

Olika moduler kan läggas till vid olika tidpunkter på ett sätt som avtalas med användaren. Den resulterande programvarusviten passar användarens specifika behov och kan ändras med tiden om användarens behov förändras.

2.2 Avsedd användning

Mjukvaran Digistat (fortsättningsvis programvara) samlar in, registrerar, organiserar, överför och visar patientinformation och patientdata, inklusive data och händelser från anslutna system och medicintekniska produkter samt information som matas in manuellt, i syfte att erbjuda ett stöd till vårdpersonalen för att diagnostisera och behandla patienter samt skapa en elektronisk journal.

- Produkten producerar en elektronisk patientdokumentation som kan konfigureras både utifrån insamlade data och information och utifrån den automatiska och manuella dokumentationen av avdelningens aktiviteter.
- Produkten tillhandahåller automatisk, sekundär visning av och ljudinformation om insamlade data, händelser, aktuell status och de anslutna systemens och medicintekniska produkternas driftförhållanden på därtill avsedda anordningar för visning. Produkten kan även konfigureras för vidareförmedling av data och information om händelser, status och driftförhållanden till Ascom meddelandesystemet.

- Produkten stöder förbättringen av sjukvårdspersonalens arbetsflöden avseende hantering av larm från anslutna system och medicintekniska produkter
- Produkten stöder dokumentationen för den föreskrivna behandlingen, dess förberedelse och administration.
- Produkten stöder registrering, validering och visning av kartlagda vitala tecken baserade på insamlade data och information.
- Produkten tillhandahåller konfigurerbara rapporter, tabeller och statistik baserade på registrerade data som ska användas av vårdpersonalen för att analysera enhetens effektivitet, produktivitet, prestanda och resursutnyttjande samt vårdkvaliteten.

Produkten ersätter **inte** eller upprepar den primära visningen av data och larm från anslutna system och medicintekniska produkter. Produkten kontrollerar **inte** och varken övervakar eller ändrar beteendet hos dessa system och medicintekniska produkter eller det larmmeddelande som är förknippat med dem.

Produkten är **inte** avsedd att användas som ett instrument för direkt diagnos eller övervakning av vitala fysiologiska parametrar.

Produkten är avsedd att användas i klinisk miljö/sjukhusmiljö av vårdpersonal med lämplig utbildning och grundar sig på att IT- och kommunikationsstrukturen vid vårdinrättningen används och fungerar korrekt och att befintliga anordningar för visning samt anslutna system och medicintekniska produkter används och fungerar korrekt.

Dessutom tillhandahåller produkten specifika funktioner och gränssnitt som är tänkta att användas av icke-professionella användare på annan plats för icke-kliniska ändamål, närmare bestämt för visning av information, rapporter, tabeller och statistik utan möjlighet att lägga till, ändra eller radera någon information eller data.

Produkten är en fristående mjukvara som installeras på servrar och datorer som måste vara i överensstämmelse med de tekniska hård- och mjukvaruspecifikationerna som levereras tillsammans med produkten.

2.2.1 Säkerhetsbestämmelser

Användaren måste grunda sina diagnos-/vårdbeslut och diagnos-/vårdningrepp uteslutande på den direkta kontrollen av den primära informationskällan. Det åligger användaren att kontrollera riktigheten hos informationen som produkten tillhandahåller och att använda denna information korrekt.

Endast utskrifter som har undertecknats digitalt eller på papper av legitimerade läkare godkänns som klinisk dokumentation. Genom att underteckna ovanstående utskrifter intygar användaren att data i dokumentet är korrekta och fullständiga.

När patientrelaterade uppgifter anges, har användaren ansvar för att verifiera att patientidentitet, hälsovårdsorganisationens avdelning / vårdarhet och den information om vårdplats som visas i Produkten är korrekt. Denna kontroll är av grundläggande betydelse vid kritiska moment som t.ex. administrering av läkemedel.

Hälsovårdsorganisationen ansvarar för att identifiera och genomföra lämpliga förfaranden för att säkerställa att potentiella fel som uppstår på Produkten och/eller vid användningen av Produkten upptäcks och åtgärdas snabbt och att de inte utgör en risk för patient eller operatör. Dessa förfaranden beror på Produkts konfiguration och den användningsmetod som föredras av hälsovårdsorganisationen.

Produkten kan beroende på konfigurationen ge åtkomst till information om läkemedel. Hälsovårdsorganisationen ansvarar för att initialts och periodiskt verifiera att denna information är aktuell och uppdaterad.

Produkten tillhandahåller inte primär avisering av larm; deb är inte avsedd att användas i stället för direkt övervakning av de larm som genereras av den medicinska utrustningen. Denna begränsning beror tillsammans med övriga anledningar på specifikationerna och begränsningarna hos de medicintekniska Produkternas kommunikationsprotokoll.

Om några av de medicintekniska Produkterna som används för Produkten är placerade inom patientområdet eller är anslutna till utrustning som är placerad inom patientområdet måste hälsovårdsorganisationen ha ansvar för att hela kombinationen överensstämmer med den internationella standarden IEC 60601-1 och eventuella ytterligare krav som fastställs i lokala bestämmelser.

Användning av Produkten måste beviljas, med hjälp av specifik konfiguration av användarkonton och aktiv övervakning av personal som är 1) utbildad enligt Produktanvisningarna av personal som har auktoriserats av tillverkaren eller tillverkarens distributörer och 2) yrkesmässigt kvalificerad att tolka Produktinformationen korrekt och vidta lämpliga säkerhetsprocedurer.

Produkten är en fristående programvara som körs på vanliga datorer och/eller mobila standardenheter som är anslutna till hälsovårdsorganisationens lokala nätverk.

Hälsovårdsorganisationen ansvarar för att tillräckligt skydda datorer, enheter och lokalt nätverk mot cyberattacker.

Produkten ska endast installeras på datorer och anordningar som uppfyller min. hårdvarukrav och endast på understödda operativsystem.

2.3 Användning "off-label" av produkte

All användning av produkten som inte anges under Avsedd användning (s.k. användning "off-label") är helt upp till användarens och den ansvariga organisationens omdöme och ansvar.

Tillverkaren garanterar överhuvudtaget inte produktens säkerhet och lämplighet om den används för andra ändamål än de som anges under Avsedd användning.



Produkten **är inte** ett primärt fördelat larmsystem.

2.4 Patientbefolkning

Produkten är en programvara och är inte i kontakt med patienten.

Patientpopulationen och patientförhållandena fastställs av medicinska enheter och system till vilka produkten är ansluten.

Utöver detta gäller följande begränsningar:

- * Patientvikt mellan 0,1 kg och 250 kg
- * Patienthöjd mellan 15cm och 250cm

2.5 Hälsovårdsorganisationens ansvar

Ascom UMS frånsäger sig allt ansvar för de konsekvenser på produktens säkerhet och funktionsduglighet som uppstår till följd av tekniska reparations- eller underhållsinsatser som inte utförs av servicepersonal eller tekniker som har auktoriserats av Ascom UMS eller auktoriserade distributörer.

Användaren och den juridiska representanten för Hälso- och sjukvårdsorganisation där utrustningen används ska göras uppmärksamma på sina ansvarsområden i enlighet med gällande lokal lagstiftning om arbetsmiljöfrågor (t.ex. italienskt lagdekret nr 81/2008) och övriga lokala säkerhetsprocedurer på arbetsplatsen.

Serviceavdelningen hos Ascom UMS och auktoriserade distributörer ger kunderna den support som krävs för att upprätthålla de levererade apparaternas säkerhet och funktionsduglighet genom att tillhandahålla rätt kunskap, instrument och reservdelar för att över tiden garantera produkternas fullständiga överensstämmelse med sina ursprungliga konstruktionsdata.



Produkten är utformad med hänsyn till de krav och bästa praxis som finns i IEC 80001-standarden och dess tillhörande tekniska rapporter. Särskilt har IEC/TR 80001-2-5:2014 stor betydelse för produkten. Som tydliggörs i IEC 80001-serien är en del av de nödvändiga aktiviteterna och riskhanteringsåtgärderna under hälso- och sjukvårdsorganisationens kontroll och ansvar. Vänligen se standarden och dess tillhörande dokumentation för att identifiera nödvändiga aktiviteter och riskhanteringsåtgärder, se särskilt aktuell giltig version av följande dokument:

- 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 Tillverkarens ansvar

Ascom UMS ansvarar för produktens säkerhet, tillförlitlighet och prestanda endast i följande fall:

- Installation och konfiguration utfördes av personal utbildad och godkänd av Ascom UMS;
- Användning och underhåll enligt instruktionerna i produktdokumentationen (inklusive den här användarhandboken);
- Användning och underhåll är i överensstämmelse med användarmanualen.
- Manualen är komplett och läslig i alla sina delar.
- Konfigurationer, ändringar och underhåll utförs endast av personal som utbildats och godkänts av Ascom UMS;

- Produktens användningsmiljö överensstämmer med gällande säkerhetsanvisningar och gällande föreskrifter;
- Miljön där produkten används (inklusive datorer, utrustning, elektriska anslutningar etc.) uppfyller gällande lokala föreskrifter.



Om produkten ingår i ett "medicinskt elsystem" genom elektrisk och funktionell anslutning till medicinsk utrustning, ansvarar hälso- och sjukvårdsorganisationen för den nödvändiga elektriska säkerhetsverifieringen och acceptanstester, även där Ascom UMS utförde helt eller delvis de nödvändiga anslutningarna.

2.7 Produktens spårbarhet

För att säkerställa enhetens spårbarhet och korrigerande åtgärder på plats, i enlighet med EN 13485 och MDD 93/42/EEC, uppmanas ägaren att informera Ascom UMS/Distributören om eventuell överlåtelse av äganderätt genom att lämna ett skriftligt meddelande om Produkten, tidigare ägare och identifikationsuppgifter för den nya ägaren.

Enhetsdata finns i Produktetiketten ("Om-rutan" som visas i produkten – se sidan **Error! Bookmark not defined.**).

Vid tvivel/frågor om Produktidentifikation, vänligen kontakta Ascom UMS/Distributörens tekniska assistans (för kontakter se sidan **Error! Bookmark not defined.**).

2.8 Uppföljningssystem efter försäljning

Den **CE** markerade enheten är föremål för eftermarknadstillsyn – vilken Ascom UMS och Distributören tillhandahåller för varje marknadsfört exemplar – gällande faktiska och potentiella risker, antingen för patienten eller för Användaren, under Produktens livscykel.

Vid försämring av enhetens egenskaper, dålig prestanda eller otillräckliga användaranvisningar som har utgjort eller kan utgöra en fara för patientens eller Användarens hälsa eller för miljösäkerheten, måste användaren omedelbart meddela antingen Ascom UMS eller Distributören.

Vid mottagande av användarfeedback påbörjar Ascom UMS/Distributören omedelbart gransknings- och verifieringsprocessen och utför nödvändiga korrigeringsåtgärder.

2.9 Produktens livslängd

Produktens livslängd beror inte på slitage eller andra faktorer som kan äventyra säkerheten. Den påverkas av programmiljöns föråldrande (t.ex. OS,.NET Framework) och är därför inställd på 5 år från Produktversionens lanseringsdatum (finns i Om-rutan).

3. Mjuk- och hårdvarudata



Digistat får endast installeras av utbildad behörig personal. Detta inkluderar Ascom UMS / distributörens personal och annan person som är särskilt utbildad och uttryckligen auktoriserad av Ascom UMS / distributören. Utan ett uttryckligt direkt godkännande från Ascom UMS / distributören har hälso- och sjukvårdsorganisationens personal inte behörighet att utföra installationsprocedurer och / eller ändra Digistat-konfigurationen.



Digistat får endast användas av utbildad personal. Digistat får inte användas utan adekvat träning, utförd av personal från Ascom UMS / distributören.

Detta kapitel listar mjuk- och hårdvaruegenskaperna som krävs för att systemet Digistat ska fungera korrekt. Informationen i detta kapitel uppfyller den informationsskyldighet som tillverkaren har enligt standard IEC 80001-1:2010 (Application of risk management for IT-networks incorporating medical devices).

Enligt standard IEC 60601-1 är det nödvändigt att använda medicinklassade anordningar om en elektrisk anordning placeras i närheten av patientsängen. I dessa situationer används vanligtvis medicinklassade PANELDATORER. På förfrågan kan Ascom UMS föreslå möjlig utrustning av denna typ.



En PDF-läsare som stöds måste installeras på arbetsstationen för att visa onlinehjälpen. Se avsnitt 3.1.3 programvarukrav för centrala arbetsstationer och arbetsstationer vid bäddarna.

3.1 Patientnära

3.1.1 Hårdvara

Min. hårdvarukrav:

- Processor Intel® I3 eller högre
- 4 GB RAM-minne (8 GB rekommenderas)
- Hårddisk med min. 60 GB ledigt utrymme
- Bildskärmsupplösning på 1024 x 768 pixlar eller högre (1920 x 1080 rekommenderas)
- Mus eller kompatibel enhet
- Gränssnitt med nätverk Ethernet 100 Mb/s (eller högre)
- CD/DVD-läsare eller möjlighet att kopiera installationsfiler

Om en central/sängkantsplacerad arbetsstation är konfigurerad för visning av videoströmmar (funktionen stöds endast i Smart Central eller OranJ med kameraintegration aktiverad) är minimikraven följande:

- Processor Intel® I3 eller högre
- Minne: 4 GB RAM + 50 MB för varje kameraström som visas samtidigt (t.ex. med 20 kameror som visas 4 GB + 1 GB)
- Hårddisk med min. 60 GB ledigt utrymme
- Bildskärmsupplösning på 1024 x 768 pixlar eller högre (1920 x 1080 rekommenderas)
- Mus eller kompatibel enhet
- Gränssnitt med nätverk Ethernet 100 Mb/s (eller högre)
- CD/DVD-läsare eller möjlighet att kopiera installationsfiler

Några exempel: med Intel i7 6600 2.60 Ghz, med en strömning av 10 kameror med en överföringshastighet på 3 138 kbps, är CPU-utnyttjandet ca 45 %. Med I3 7100t 3,4 Ghz, med en strömning av 16 kameror med en överföringshastighet på 958 kbps, är CPU-utnyttjandet ca 30 %.

3.1.2 Operativsystem

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

3.1.3 Systemmjukvara

- Microsoft Framework .NET 4.5
- Adobe Acrobat Reader 10

NOTERA: Produktens användarhandbok är en PDF-fil framtagen enligt PDF-standard med version 1.5 och kan därmed läsas av Adobe Acrobat 6.0 eller senare. Vidare testades produktens användarhandbok med Adobe Acrobat Reader 10. Sjukhusorganisationen kan använda en annan version av Acrobat Reader: Verifieringen av den installerade produkten kommer att innefatta kontrollen av att användarhandboken är korrekt läsbar.

3.2 Server

3.2.1 Hårdvara

Minsta hårdvarukrav (liten installation, 20 bäddar, 4 enheter vardera):

- Intel® I5-processor med 4 kärnor.
- 4 GB RAM-minne (8 GB rekommenderas)
- Hårddisk med min. 120 GB ledigt utrymme
- Gränssnitt med nätverk Ethernet 100 Mb/s (eller högre). 1 Gb/s rekommenderas.
- CD/DVD-läsare eller möjlighet att kopiera installationsfiler

Rekommenderade hårdvarukrav (medelstor installation, 100 bäddar, 4 enheter vardera, Connect och Mobile):

- Intel® I7-processor med 8 kärnor
- 32 GB RAM-minne
- Hårddisk med min. 120 GB ledigt utrymme
- Gränssnitt med nätverk Ethernet 1 Gb/s
- CD/DVD-läsare eller möjlighet att kopiera installationsfiler

3.2.2 Operativsystem

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

3.2.3 Systemmjukvara

- 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 har testats på Ascom Myco SH1 och SH2 Wi-Fi och Mobila Smartphone-enheter, med Android-version 4.4.2 (Myco1) eller 5.1 (Myco2) eller 8.0 (Myco3). Det är därför kompatibelt med Myco1, Myco2 och Myco3-mobila enheter.

Programmet är utformat för att vara kompatibelt med andra Android-enheter med en minsta skärmstorlek på 3,5”; kompatibilitet med en viss enhet måste verifieras före klinisk användning.

Kontakta Ascom UMS för den kompletta listan över enheter som stöder Digistat Mobile.

3.4 Digistat “Web”

Följande webbläsare stöds för användning med Digistat webbapplikationer:

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



Endast stödda webbläsare kommer att användas för Digistat Web.



En Digistat Web-arbetsstation har alltid webbläsaren i förgrunden. Dessutom kommer webbläsaren aldrig att användas för något annat än Digistat Web (vilket innebär att Digistats webbsida kommer att vara webbsidans standardwebbplats).



Webbläsarens bildskalning ska alltid vara inställd på 100%.



När det lokala nätverket är åtminstone delvis baserat på WiFi-anslutningar, kan de intermittenta egenskaperna hos WiFi-anslutningar, kopplingar uppstå och systemet kanske inte är tillgängligt. Hälso- och sjukvårdsorganisation måste fungera för att säkerställa optimal WiFi-täckning och instruera personalen om hur man hanterar dessa tillfälliga systemavbrott.

3.5 Varningar



Programmet "MDI Web" som presenteras i den relevanta Användarmanualen kan endast användas för demonstrationsändamål. Det kan inte användas i produktionsmiljö.



För att använda Digistat korrekt är det nödvändigt att Microsoft Windows bildskärmsskalning är inställd på 100 %. Andra inställningar kan hindra produktens funktion eller ge felfunktioner på diagramnivå. Se Microsoft Windows dokumentation för värdet för bildskärmsskalning



Min. upplösning i vertikalled på 768 stöds endast om Digistat har konfigurerats för att köras med helskärm eller när Windows-raden är konfigurerad för att döljas automatiskt (Auto-hide).



De datorer och andra anordningar som används ska vara anpassade för användningsmiljön. De ska därför uppfylla gällande standarder och bestämmelser.



Det är obligatoriskt att följa tillverkarens anvisningar för förvaring, transport, installation, underhåll och borttagning av tredjepartshårdvara. Dessa moment får endast utföras av behörig personal med rätt kunskaper.



Användning av produkten tillsammans med någon annan programvara än den som specificeras i detta dokument kan äventyra produktens säkerhet, effektivitet och designkontroller. Sådan användning kan leda till en ökad risk för användare och patienter. Det är obligatoriskt att rådfråga en auktoriserad tekniker från Ascom UMS eller distributören innan någon annan programvara än den som specificeras i detta dokument används tillsammans med produkten.

Om hårdvaran som produkten körs på är en fristående dator ska inte användaren installera någon annan programvara (tilläggsprogram eller applikationsprogram) på datorn. Det rekommenderas att tillämpa en tillståndspolicy som förhindrar att användare utför procedurer såsom installation av ny programvara.



Ansvarig inrättning ska implementera en mekanism för synkronisering av datumet och tiden för arbetsstationerna, på vilka Digistat körs, med en referenstidskälla.



Det rekommenderas att inaktivera åtkomst till Internet på klientarbetsstationerna och de handhållna enheter som produkten

	används på. Alternativt ska hälso- och sjukvårdsorganisationen införa nödvändiga säkerhetsåtgärder för att garantera ett adekvat skydd mot cyberangrepp och installation av obehöriga applikationer.
	Delar av produkten fungerar som visare av videoströmmar; Produkten är inte källan till videoströmmen och den registrerar inte denna information på något sätt. Det är hälsovårdsorganisationens ansvar att hantera systemet från ett dataskyddsperspektiv, inklusive installation och konfiguration av källkameror.
	Delar av Produkten hanterar ljud och bild relaterade till användarna och/eller patienterna inklusive förvärv, bearbetning och inspelning. Det är hälsovårdsorganisationens ansvar att genomföra de nödvändiga förfarandena för att följa den lokala dataskyddsförordningen. Inklusive men inte begränsat till definition av användningsbegränsningar och utbildning av användare.
	Funktionen för videoströmning på stationära arbetsstationer har testats med H264- och H265-videokodek. Eventuell annan videokodek som är ursprungligt närvarande eller installerad av tredjepartsapplikationer (t.ex. VLC Media Player) måste testas före användning.
	Varning: varje videokälla stöder ett maximalt antal samtidigt anslutna klienter. Det är hälsovårdsorganisationens ansvar att avgöra det högsta antalet och informera användarna.
	Funktionen för videoströmning på mobila enheter stöder endast RTSP-videoströmmar med följande autentiseringstyper: • Ingen autentisering; • Grundläggande autentisering; • Sammandragen autentisering;
	Funktionen för videoströmning på mobila enheter stöder endast H263-, H264- och H265-videokodek.

3.6 Brandvägg och virusskydd

Följande är nödvändigt för att skydda systemet Digistat från möjliga IT-angrepp:

- Windows brandvägg är aktiv både på arbetsstationer och server.
- En mjukvara för viruss/malware kydd är aktiv och regelbundet uppdaterad på arbetsstation och server.

Ansvarig organisation ska se till att dessa två skydd finns. Ascom UMS har testat produkten med F-SECURE virusskydd. Hänsyn måste dock tas till vårdenheten befintliga val och policy. Valet av det specifika virusskyddet överläts åt ansvarig

organisation. Ascom UMS kan inte garantera att systemet Digistat är kompatibelt med alla virussydd eller virussyddets konfiguration.



Inkompatibilitet med delar av produkten Digistat systemets har signalerats vid användning av Kaspersky virussydd. Åtgärdandet av detta har krävt definition av specifika regler i virussyddet.



Det rekommenderas starkt att endast bibehålla de TCP- och UDP-portar öppna som verkligen behövs. De kan variera beroende på konfigurationen av systemet. Det rekommenderas därför att kontakta teknisk service för all aktuell information.

3.6.1 Ytterligare rekommenderade försiktighetsåtgärder för cyberskydd

För att ytterligare skydda Digistat -systemet från möjliga cyberangrepp rekommenderas det starkt att:

- planera och genomföra en "härdning" av IT-infrastrukturen inklusive IT-plattformen som utgör runtimemiljön för produkten,
- implementera ett intrångsdetekterings- och förebyggande system (IDPS),
- utföra ett penetrationstest och, om någon svaghet upptäcks, utföra alla nödvändiga åtgärder för att minska risken för cyberintrång,
- avvisa enheterna när de inte längre kan uppdateras,
- planera och utföra en periodisk verifiering av integriteten hos filer och konfigurationer,
- implementera en DMZ-lösning (demilitarized zone) för webbservrar som behöver exponeras på internet.

3.7 Det lokala nätverkets egenskaper

I detta avsnitt listas de egenskaper som krävs för det lokala nätverket i vilket Digistat systemet är installerat för att systemet ska fungera korrekt.

- Digistat systemet använder TCP/IP-baserad trafik.
- Det lokala nätverket (LAN) måste vara fritt från flaskhalsar.
- Digistat systemet kräver att det finns minst ett 100 Megabit LAN för klientens arbetsstation. 1 Gigabit Ethernet stamnät är eftersträvänsvärt.
- Det får inte finnas filter på TCP/IP-trafiken mellan arbetsstationer, servrar och sekundära anordningar.
- Om anordningarna (servrar, arbetsstationer eller sekundära anordningar) är anslutna till olika undernätverk måste det finnas routing mellan dessa undernätverk.
- Det rekommenderas att använda redundansteknik för att säkerställa nätverkstjänsten även i händelse av felfunktion.
- Det rekommenderas att schemalägga underhållskalendern tillsammans med Ascom UMS/distributörerna för att Ascom UMS eller den auktoriserade distributören effektivt ska kunna stödja vårdenheten i hanteringen av eventuella störningar som orsakas av underhållsåtgärder.



Om nätverket inte har rätt egenskaper sker en gradvis hastighetsminskning hos produkten tills det uppstår timeoutfel på åtkomsten till data, d.v.s. tills läge Recovery nås.



Om det används ett WiFi-nät kan det, p.g.a. upprepade avbrott hos WiFi-anslutningen, förekomma nätfrånkopplingar som medför att Recovery Mode aktiveras och att det saknas åtkomst till systemet. Ansvarig organisation måste vidta åtgärder för att garantera en optimal täckning och stabilitet hos WiFi-nätet och utbilda berörd personal i hur dessa tillfälliga frånkopplingar ska hanteras.



För att kryptera data som överförs via trådlösa nätverk rekommenderas det att anta det högsta säkerhetsprotokollet tillgängligt, aldrig mindre än WPA2.

3.7.1 Digistat systemets inverkan på vårdenhetens nätverk

Digistat systemet inverkar på vårdenhetens lokala nätverk. Detta avsnitt innehåller information om trafiken som genereras på nätverket av Digistat systemet så att strukturen kan utvärdera och analysera riskerna som är förknippade med införandet av Digistat systemet.

Bandbredden som används av ett Digistat-system beror på många olika faktorer. De viktigaste är:

- Antalet arbetsstationer.
- Antalet arbetsstationer som konfigureras som centrala stationer.
- Antalet och typen av enheter avsedda för datainsamling.
- Gränssnitt med externa system.
- Digistat systemets konfiguration och användningssätt.

Digistat bandbredd yrke beror huvudsakligen på datainsamling från medicintekniska produkter. I en konfiguration med förvärv på 100 bäddar där varje säng samlar data från 1 ventilator, 1 patientmonitor och 3 infusionspumpar och med 10 Digistat arbetsstationer som visar 10 bäddar varje kan användningen av bandbredd uppskattas som följer.

Genomsnitt: 0,8 – 6 Mbit/s

Max: 5 – 25 Mbit/s

I händelse av Digistat konfigurationer utan förvärv från medicinska anordningar, bandbreddsockupations värden är lägre än de som anges ovan.

4. Före användning

4.1 Varningsföreskrifter för installation och underhåll

Följande varningsföreskrifter avseende korrekt installation och underhåll av produkten DIGISTAT ska följas noggrant.



Installation, underhåll och reparationer ska utföras i enlighet med Ascom UMS-procedurer och -instruktioner och endast av Ascom UMS / distributörens tekniker eller personal utbildad och godkänd av Ascom UMS / distributören.



Det rekommenderas att hälso- och sjukvårdsorganisationen som använder produkten att fastställa ett underhållsavtal med Ascom UMS eller en auktoriserad distributör. En del av underhållet ska innehålla uppgradering till den senaste versionen av produkten.

Kom ihåg att DIGISTAT systemet endast får installeras och konfigureras av utbildad och auktoriserad personal. Detta omfattar personal från Ascom UMS eller auktoriserade distributörer eller annan specialutbildad personal som är auktoriserad av Ascom UMS eller distributörerna.

På samma sätt får underhåll och reparation av DIGISTAT systemet endast utföras av utbildad och auktoriserad personal i enlighet med företagets procedurer och riktlinjer. Detta omfattar personal från Ascom UMS eller distributörerna eller annan specialutbildad personal som är auktoriserad av Ascom UMS eller distributörerna.



DIGISTAT systemet får endast installeras och konfigureras av utbildad och auktoriserad personal. Detta omfattar personal från Ascom UMS eller auktoriserade distributörer eller annan specialutbildad personal som är auktoriserad av Ascom UMS eller distributörerna.

- Använd tredjepartsenheter som rekommenderas av Ascom UMS/distributörerna.
- Endast utbildade och auktoriserade personer får installera tredjepartsenheter.
- Felaktig installation av tredjepartsenheter kan medföra en risk för personskada för patient och/eller operatörer.
- Följ ytterst noggrant tillverkarens instruktioner för installation av tredjepartshårdvaran.
- Utför regelbundet underhåll av systemet enligt instruktionerna i denna manual och de som medföljer tredjepartsenheterna.

- Hälsovårdsorganisationen ansvarar för att välja utrustning som är lämplig för miljön i vilken den installeras och används. Hälsovårdsorganisationen bör bland annat överväga elsäkerhet, EMC-strålning, störning av radiosignaler, desinfektion och rengöring. Uppmärksamhet ska ges till enheter installerade i patientområdet

4.2 Försiktighetsåtgärder och varningsföreskrifter



Garanterar mjukvarans tillförlitlighet och säkerhet under användningen genom att noggrant följa anvisningarna i detta kapitel av manualen.



Hälso- och sjukvårdsorganisationerna säkerställa att underhållet av produkten och tredjepartsenheten implementeras på efterfrågat sätt för att garantera säkerheten och effektiviteten samt minska risken för funktionsfel och att det uppstår eventuella faror för patienten och användaren.



Produkten ska endast användas av utbildade och auktoriserade läkare.

4.3 Integritetspolicy

Lämpliga försiktighetsåtgärder ska vidtas för att skydda användarnas och patienternas integritet, och för att säkerställa att personuppgifter behandlas genom att respektera de registrerades rättigheter, grundläggande friheter och värdighet, särskilt när det gäller sekretess, personlig integritet och rätten till personuppgifters skydd.



Med 'personuppgifter' menas all information som rör en identifierad eller identifierbar fysisk person ('registrerad'); en identifierbar fysisk person är en som kan identifieras direkt eller indirekt, särskilt med hänvisning till en identifierare såsom ett namn, ett identifikationsnummer, platsdata, en onlineidentifierare eller en eller flera faktorer som är specifika för fysiska, fysiologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identiteten hos den fysiska personen.

Särskild uppmärksamhet ska ägnas åt de uppgifter som definieras i "EU:s allmänna dataskyddsförordning 2016/679 (GDPR)" som "Särskilda kategorier av personuppgifter".

Särskilda kategorier av personuppgifter:

(...) Personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska övertygelser eller fackligt medlemskap och (...) genetiska data, biometriska data i syfte att identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexliv eller sexuell läggning.

Hälso- och sjukvårdsorganisationen måste försäkra sig om att användningen av produkten överensstämmer med kraven i tillämplig förordning om integritet och skydd av personuppgifter, särskilt i enlighet med hanteringen av ovan nämnda uppgifter.

Digistat hanterar följande personuppgifter:

- Förnamn och efternamn
- Födelsedatum
- Kön
- Patientkod
- Inskrivningsdatum
- Utskrivningsdatum
- Patientvikt
- Patientlängd

Digistat kan konfigureras att automatiskt dölja dessa data på varje applikationsskärm. För att göra det, ställ in systemalternativet "Integritetsläge" till "Sant" i Digistat-konfigurationstillämpningen, (se Digistat-konfigurations- och installationshandboken för detaljerad procedur). Standardvärdet är "Sant".

Om alternativet "Sekretessläge" är satt till sant är följande fall möjliga:

- utan att någon användare är inloggad visas ingen patientinformation.
- med en användare inloggad, och användaren inte har något särskilt tillstånd visas ingen patientinformation.
- med en användare inloggad och användaren har ett särskilt tillstånd visas patientinformation.

Alternativet kan tillämpas på en enskiöld arbetsstation (dvs. olika arbetsstationer kan konfigureras olika).



Läs noggrant försiktighetsåtgärderna i detta avsnitt och följ dem omsorgsfullt.

- De datorer som används får inte lämnas obebakade och tillgängliga under arbetspassen med Digistat. Det rekommenderas att logga ut från systemet när du lämnar arbetsstationen.
- Personuppgifter som matas in i systemet såsom lösenord eller personuppgifter för användare och patienter ska skyddas mot alla former av försök till oauktoriserad åtkomst genom lämpliga mjukvaror (virusskydd och brandvägg). Vårdenheten är ansvarig för att implementera denna mjukvara och hålla den uppdaterad.



Personuppgifter kan finnas i några rapporter från Digistat. Hälso- och sjukvårdsorganisationen behöver hantera dessa dokument enligt gällande standarder för integritet och personuppgifter.



Klientarbetsstationer (både skrivbord och mobil) lagrar inte patientdata på disken. Patientdata lagras endast inuti databasen och databaslagring beror på sjukvårdsstrukturens procedurer och val (exempel: fysisk maskin, SAN, virtualiseringsmiljö). Patientdata ska behandlas enligt alla gällande standarder för integritet och personuppgifter.



Patientdata lagras inte i proprietära filer. Den enda platsen där patientdata lagras är databasen.



Under vissa omständigheter överförs personliga data i okrypterat format med en anslutning utan innbyggd säkerhet. Ett exempel på denna situation är kommunikation med protokollet HL7. Det åligger ansvarig organisation att tillämpa säkerhetsmekanismer inom sjukhusets nätverk som garanterar att gällande lagar och bestämmelser om sekretesspolicy uppfylls.



Det föreslås att konfigurera databasservern så att Digistat-databasen krypteras på disken. För att aktivera detta alternativ krävs SQL Server Enterprise Edition och under installationen är det nödvändigt att aktivera alternativet TDE (Transparent Data Encryption).



Hälso- och sjukvårdsorganisationen har ansvaret för grundläggande utbildning avseende integritetsfrågor: dvs. grundläggande principer, regler, föreskrifter, ansvarsområden och sanktioner i den specifika arbetsmiljön.

Ascom UMS / distributören ska tillhandahålla specialiserad utbildning om bästa möjliga användning av produkten som rör integritetsfrågor (dvs. databasanonymisering, sekretessläge, användarrättigheter etc.).



Hälso- och sjukvårdsorganisationen ska producera och behålla följande dokumentation:

- 1) den uppdaterade listan över systemadministratörer och underhållspersonal;
 - 2) de undertecknade blanketterna för tilldelning och certifieringen av närvaro vid utbildningen;
 - 3) ett register över behörigheter, tillstånd och privilegier som beviljats användarna;
 - 4) en uppdaterad lista över produktanvändarna.
-



Hälso- och sjukvårdsorganisationen ska genomföra, testa och intyga ett förfarande för automatisk avaktivering av inte längre aktiva användare efter en viss period.



Hälso- och sjukvårdsorganisationen ska kodifiera, införa och dokumentera ett förfarande för periodisk verifiering av att tillhöra rollen som systemadministratör och teknisk underhållspersonal.



Hälso- och sjukvårdsorganisationen ska genomföra revisioner och kontroller av operatörernas korrekta beteende.



Databaser som innehåller patientdata / känsliga uppgifter kan inte lämna vårdinrättningen utan att krypteras / avidentifieras.

4.3.1 Användning av användarens inloggningsuppgifter och dess egenskaper

Detta avsnitt förklarar Digistat autentiseringsuppgifternas (användarnamn och lösenord) egenskaper, deras användning och rekommenderade policy.

- Varje användare ska vidta samtliga nödvändiga försiktighetsåtgärder för att hemlighålla användarnamnet och lösenordet.
- Användarnamn och lösenord är privata och personliga. Berätta aldrig ditt användarnamn och lösenord för någon annan.
- Varje användare kan ha en eller flera inloggningsuppgifter för att identifiera sig (användarnamn och lösenord). Samma användarnamn och lösenord får inte användas av flera användare.
- Behörighetsprofilerna ska kontrolleras och förnyas minst en gång om året.
- Det går att gruppera olika behörighetsprofiler utifrån hur likartade användarnas arbetsuppgifter är.
- Varje användarkonto ska förknippas med en specifik person. Användning av allmänna användare (t.ex. ADMIN eller SKÖTERSKA) ska undvikas. Av spårbarhetsskäl är det m.a.o. nödvändigt att varje användarkonto endast används av en användare.
- Samtliga användare har en tilldelad auktorisationsprofil som endast ger dem åtkomst till de funktioner som är relevanta för deras arbetsuppgifter. Systemadministratören ska tilldela lämplig profil samtidigt som användarkontot skapas. Denna profil ska ses över minst en gång om året. Denna översyn kan även ske för klasser av användare. Procedurerna för definition av användarprofilen beskrivs i manualen för konfiguration av Digistat.
- Lösenordet ska bestå av minst åtta tecken.
- Lösenordet får inte innehålla uppgifter som lätt kan härledas till användaren (t.ex. förnamn, efternamn, födelsedatum o.s.v.).
- Lösenordet tilldelas av systemadministratören och ska ändras av användaren när systemet används första gången.
- Därefter ska lösenordet ändras minst en gång var tredje månad.
- Om inloggningsuppgifterna (användarnamn och lösenord) inte används på över sex månader måste de deaktiveras. Undantaget från detta är specifika användaruppgifter som används för tekniskt underhåll. Se den tekniska

manualen om Digistat för procedurerna för konfiguration av denna egenskap.

- Inloggningsuppgifterna måste deaktiveras även när användaren förlorar sin kvalifikation att använda uppgifterna (t.ex. när en användare flyttar till en annan avdelning). Systemadministratören kan aktivera/deaktivera en användare manuellt. Proceduren beskrivs i manualen för konfiguration av Digistat.

Följande information riktar sig till systemadministratörer:

Lösenordet måste respektera ett reguljärt uttryck som definieras i konfigurationen av Digistat (standard är ^.....* d.v.s. åtta tecken).

Systemadministratören tilldelar lösenordet när det skapas ett nytt konto för en användare. Systemadministratören kan tvinga användaren att ändra lösenordet vid den första åtkomsten till systemet. Lösenordet förfaller efter en konfigurerbar tidsperiod. Användaren måste ändra lösenordet när denna tidsperiod har förflutit. Det går att göra så att en användares lösenord inte förfaller.

Se manualen för konfiguration av Digistat för detaljerad information om definitionen av användarkontona och konfigurationen av lösenordet.

4.3.2 Systemadministratörer

I samband med normal installation, uppdatering och teknisk service av mjukvaran Digistat kan personal från Ascom UMS eller auktoriserade distributörer få åtkomst till och behandla personuppgifter och känsliga data som finns lagrade i databasen för Digistat.

Ascom UMS eller distributören tillämpar i samband med hanteringen och behandlingen av personuppgifter och känsliga data de arbetsprocedurer och -instruktioner som är i överensstämmelse med gällande personuppgiftslagstiftning ("General Data Protection Regulation - EU 2016/679").

Vid ovannämnda aktiviteter agerar personalen från Ascom UMS eller distributören som Systemadministratör för systemet Digistat (se Personskyddsmyndighetens åtgärd om systemadministratörer av 25 november 2008). Personalen som har utsetts av Ascom UMS eller distributören att utföra dessa aktiviteter har rätt kunskaper om de försiktighetsåtgärder som gäller för sekretessen och i synnerhet för behandlingen av känsliga data.

För att uppfylla kraven i systemadministratörernas bestämmelser måste ansvarig organisation:

- definierar åtkomsterna med namn;
- aktiverar loggen för åtkomsterna på operativsystemnivå både på servern och på klienterna;

- aktiverar loggen för åtkomsterna till databaseservern Microsoft SQL Server (Audit Level);
- konfigurerar och hanterar båda dessa loggar så att det går att spåra åtkomsterna under minst ett år.

4.3.3 Systemloggar

Digistat registrerar systemloggarna i databasen. Dessa loggar sparas en tidsperiod som är konfigurerbar. Loggarna sparas olika tidsperioder beroende på sin karaktär. Följande tidsperioder är standard:

- informationsloggarna sparas i 10 dagar;
- varningsloggarna sparas i 20 dagar;
- felloggarna sparas i 30 dagar.

Dessa tidsperioder kan konfigureras. Se manualen för konfiguration för proceduren för definition av vilka tidsperioder loggarna ska sparas.

4.3.4 Forensisk logg

En delmängd av de tidigare nämnda systemloggar, definierade enligt policyn för varje specifik sjukvårdsstruktur som använder produkten som "kliniskt relevant" eller "kliniskt användbar", kan skickas till ett externt system (antingen SQL-databas eller Syslog) för lagring enligt behoven och reglerna hos sjukvårdsstrukturen.

4.4 Säkerhetskopieringspolicy



Det rekommenderas att regelbundet säkerhetskopiera produktdatabasen.

Hälso- och sjukvårdsorganisation som använder Digistat systemet måste definiera en säkerhetskopieringspolicy som bäst passar dess datasäkerhetskrav.

Ascom UMS eller den auktoriserade distributören erbjuder sin hjälp för att implementera den definierade policyn.

Hälso- och sjukvårdsorganisation måste säkerställa att säkerhetskopiefiler lagras på ett sätt som gör att de omedelbart finns tillgängliga vid behov.

Om data lagras på borttagbara minnesenheter ska Hälso- och sjukvårdsorganisation skydda dessa enheter från oauktoriserad åtkomst. När dessa enheter inte används längre måste de antingen raderas på ett säkert sätt eller förstöras.

4.5 Procedur vid funktionsfel



Det rekommenderas att utföra säkerhetskopiering av arbetsstationens hårddisk, så att det vid ett byte ut maskinvaran är möjligt att snabbt återställa driftsmiljön.



Det rekommenderas att regelbundet utföra säkerhetskopieringar av Digistat-data.

Detta avsnitt beskriver den policy som föreslås av Ascom UMS om det uppstår ett funktionsfel i en Digistat arbetsstation. Målet med proceduren är att minimera tiden som krävs för att ersätta arbetsstationen med funktionsfel på ett korrekt sätt.

Ascom UMS föreslår att det ska finnas till hands en extra dator (ersättningsutrustning) på vilken Digistat redan har installerats.

I händelse av funktionsfel i en Digistat arbetsstation kan ersättningsutrustningen snabbt avlösa Digistat arbetsstationen.

Tänk alltid på att Digistat endast får installeras av utbildad och auktoriserad personal. Detta omfattar personal från Ascom UMS/distributörer och personer med särskild utbildning och som uttryckligen har auktoriserats av Ascom UMS/distributören. Om en uttrycklig och direkt auktorisation från Ascom UMS/distributören saknas får sjukhuspersonalen inte utföra installationsprocedurer och/eller ändra konfigurationen av Digistat.

Risken med deaktiveringen och ersättningen av Digistat arbetsstationen är att arbetsstationen förknippas med fel patientsäng eller sal. Detta kan leda till patientförväxling som är ett extremt farligt tillstånd.

Risken med ersättningen och/eller omkonfigurationen av nätverksutrustningen som är involverad i Digistat datainsamlingen (d.v.s. portserver, dockningsstation o.s.v.) är att insamlade data tilldelas fel patient. Insamlade data gällande patienten baseras på

IP-adressen för Digistat arbetsstationen. Om den ändras kan det antingen leda till att dataflödet avbryts eller (i allvarliga fall) att data tilldelas fel patient.



Felfunktion hos arbetsstationen och ersättning av denna är potentiellt farliga. Med anledning av detta får ersättningen under alla omständigheter endast utföras av auktoriserad och utbildad personal.

Risken med denna procedur är att fel bädd/sal/domän tilldelas arbetsstationen, vilken då visar data som inte tillhör de aktuella patienterna/bäddarna.

Om en Digistat-arbetsstation måste deaktiveras och ersättas ska sjukhuspersonalen omedelbart kontakta Ascom UMS (eller auktoriserade distributörer) och beställa en sådan åtgärd.

Ascom UMS föreslår att vårdenheten fastställer en klar, entydig arbetsprocedur och informerar all berörd personal om denna procedur.

För att förkorta ersättningstiderna föreslår Ascom UMS att vårdenheten har en eller flera ersättningsutrustningar till hands med alla nödvändiga program (OS, brandvägg, antivirus, RDP o.s.v.) och Digistat systemet redan installerade, men deaktiverade (d.v.s. de kan inte köras av någon användare utan hjälp av en tekniker från Ascom UMS). Vid ett eventuellt funktionsfel hos en Digistat arbetsstation garanterar tillgången till ersättningsutrustning att återställningstiderna minimeras (ersättning av hårdvara) och reducerar risken för att patientdata förknippas felaktigt.

Vid ett eventuellt funktionsfel hos en Digistat arbetsstation föreslår vi att följande procedur utförs om en ersättningsutrustning finns till hands:

- 1) Vårdenhetens auktoriserade personal byter ut datorn med felfunktion mot ersättningsutrustningen.
- 2) Vårdenhetens personal kontaktar Ascom UMS/distributören och ber om aktivering av ersättningsutrustningen.
- 3) Personalen hos Ascom UMS/distributören deaktiverar arbetsstationen med funktionsfel och konfigurerar ersättningsutrustningen korrekt.
- 4) Datorn med felfunktion repareras och görs i ordning för att fungera som ersättningsutrustning.

Anvisningarna för hur en Digistat-arbetsstation aktiveras/deaktiveras och ersätts (reserverat för systemadministratörerna) finns i Digistat konfigurationsmanual.

4.5.1 Omkonfiguration eller utbyte av apparat i nätverket

Om det är nödvändigt att antingen omkonfigurera eller ersätta en nätverksenhet som är inblandad i Digistat datainsamlingen ska vårdenhetens personal omedelbart kontakta Ascom UMS/distributören och schemalägga ersättnings-/omkonfigurationsproceduren så att personal från Ascom UMS antingen kan omkonfigurera Digistat eller ge all nödvändig information till vårdenheten. Det

rekommenderas för detta ändamål att fastställa en tydlig procedur och dela den med all inblandad personal. Några allmänna anvisningar om denna finns i Digistat konfigurationsmanual.

4.6 Förebyggande underhåll



Det rekommenderas att regelbundet utföra säkerhetskopieringar av Digistat-data.

Det rekommenderas att utföra underhåll av systemet Digistat minst en gång om året. Underhållsintervallen måste fastställas utifrån hur komplicerat systemet är. Om systemet är mycket komplicerat rekommenderas det att utföra underhållet oftare, upp till två gånger om året.

Se manualen för Produktinstallation och -konfiguration för kontrollistan för underhåll.

•

4.7 Kompatibla enheter

Kontakta Ascom UMS/distributören för en lista över tillgängliga drivrutiner.



Produkten är inte utformad för att kontrollera att enheterna fungerar korrekt utan snarare för att samla in och katalogisera kliniska data.



Insamlingen av data på Produkten avbryts om en enhet fränkopplas under körningen. Data från enheterna som går förlorade under fränkopplingen återhämtas inte av Produkten efter återanslutningen.



Avaktivera aldrig larmmeddelandet på medicinsk utrustning, om inte uttryckligen tillåtet av den medicintekniska tillverkarens dokumentation och sjukvårdsorganisationens förfarande.



Korrektheten hos parametrar som visas av Produkten måste alltid dubbelkontrolleras på den ursprungliga medicinska enheten som genererade dem.



Ljudet får aldrig deaktiveras på arbetsstationerna på vilka Produkten körs.



Av orsaker som ligger utanför programvarans kontroll, till exempel, hur de fysiska enheterna är installerade / kablade är förseningar möjliga mellan larmgenerationen och den faktiska larmdisplayen.



Om den generiska Alaris® drivrutinen används är det nödvändigt att vänta i minst 10 sekunder efter att en infusionspump har fränkopplats innan en annan infusionspump ansluts.



Uppdateringen av data som visas på skärmbilden i samband med anslutning, avstängning, fränkoppling och ändring av enhetens status beror på den tid som enheten behöver för att kommunicera ändringarna. Denna tid beror på olika faktorer. Bland dem ingår typen av enhet och typen av anslutning. Det förekommer tillstånd då

tidsfördröjningen av kommunikationen av ändringarna kan vara markanta för vissa enheter. Eftersom tillstånden kan variera beroende på enheternas konfiguration och driftförhållanden går det inte att ange tidsfördröjningarna för alla slags enheter.



Drivenheterna som används för att läsa av data från de anslutna medicintekniska produkterna har en avläsningscykel på mindre än 3 sekunder (d.v.s. alla data från enheterna läses av minst var 3:e sekund). Det finns dock enheter som kommunicerar informationen mer sällan (5–10 sekunders intervall). Se drivenhetens specifika dokumentation för detaljer om avläsningscykeln.

I en testmiljö som är installerad och konfigurerad som angivet i "Digistat-serverinstallations- och konfigurationshandboken", så snart en drivrutin upptäcker ett larm, tar det högst 1 sekund att överföra det till Produkten.



I samband med ett strömavbrott tar det några minuter för systemet att vara driftklart igen och genererar därför larmmeddelanden (vanligtvis är denna tid kortare än 3 minuter men det beror på de använda datorernas konfiguration).

4.8 Otillgängligt system

Om det under startfasen uppstår problem med att ansluta sig till servern meddelar systemet detta med en skärmbild.

Anslutningsproblemet kan inom kort lösas på egen hand. Kontakta i motsatt fall teknisk support. Se sid. 37 för listan med kontaktuppgifter.

Det finns sällsynta extremfall när det är fysiskt omöjligt att använda systemet Digistat (t.ex. naturkatastrofer, långvariga strömbrott o.s.v.).

Organisationen som använder Digistat ska ta fram en nödprocedur att följa i dessa fall. Detta för att

- 1) avdelningarna ska kunna fortsätta att utföra sin verksamhet,
- 2) snarast möjligt återställa åtkomsten till systemet (säkerhetskopieringspolicyn är en del av denna hantering, se avsnitt 4.4).



Strukturen som använder Digistat ska ta fram en nödprocedur att följa när det saknas åtkomst till systemet.

Ascom UMS eller distributören erbjuder sin hjälp för att ta fram denna procedur.

Se avsnitt 5 och följande för listan med kontaktuppgifter.

5. Tillverkarens kontaktuppgifter

Kontakta vid eventuella frågor först och främst distributören som installerade produkten.

Här är tillverkarens kontaktuppgifter:

Ascom UMS s.r.l. Unipersonale

Via Amilcare Ponchielli 29, IT-50018 Scandicci (FI), Italien

Tfn (+39) 055 0512161

Fax (+39) 055 8290392

Teknisk service

support.it@ascom.com

800999715 (gratisnummer, endast Italien)

Försäljnings- och produktinformation

it.sales@ascom.com

Allmän information

it.info@ascom.com

6. Kvarstående risker

En riskhanteringsprocess har implementerats i livscykeln för Digistat [SI1] enligt relevanta tekniska standarder (EN 14971, EN 62304 och EN 62366). Riskkontrollåtgärder har identifierats och implementerats för att reducera de kvarstående riskerna till den lägsta nivån och göra dem acceptabla jämfört med fördelarna med produkten. Den totala kvarstående risken är också acceptabel jämfört med samma fördelar.

De kvarstående riskerna som listas nedan har tagits med i beräkningen och reducerats till den lägsta möjliga nivån. De kan inte elimineras helt p.g.a. det inneboende riskkonceptet. Det är därför enligt standarderna nödvändigt att göra användarna medvetna om samtliga möjliga risker (om än avlägsna).

- Oförmåga att använda Digistat eller några av dess funktioner som förväntat, vilket kan orsaka förseningar och/eller fel i terapeutiska/diagnostiska åtgärder.
- Obehöriga åtgärder som utförs av användare, vilka kan orsaka fel i terapeutiska/diagnostiska åtgärder och i ansvarsfördelningen av dessa åtgärder
- Oavsiktlig radering av data med påföljande förlust av data, vilket kan orsaka förseningar och / eller fel i terapeutiska / diagnostiska åtgärder.
- Felaktig hantering av patientdata, inklusive fel vid visualisering, tillägg, modifiering och radering av data som kan orsaka förseningar och/eller fel i terapeutiska/diagnostiska åtgärder.
- Oavsedd användning av Digistat (t.ex. produkten används som system för primär avisering av larm, terapeutiska eller diagnostiska beslut och ingripande uteslutande baserade på informationen tillhandahållen av Produkten).
- Obehörigt avslöjande av användare och/eller patientens personuppgifter.

RISKER AVSEENDE HÅRDVARAN SOM ANVÄNDS FÖR DEN MEDICINTEKNISKA PRODUKTEN

- Elchock för patienten och/eller användaren, vilket kan orsaka personskada och/eller dödsfall för patienten/användaren.
- Överhettning av hårdvarukomponenter som kan orsaka personskada för patienten/användaren.
- Infektionssmitta för patienten/användaren.