Dentsply Sirona THE DENTAL SOLUTIONS COMPANY™

Sidexis 4

Datenschutz und Produktsicherheit

Whitepaper

Inhalt

1 EINLEITUNG 6

Zweck des Dokuments 7

2 DATENSCHUTZ 9

Definitionen für Datenschutz laut DSGVO 9
Grundsätze für Datenschutz 10
Datenschutz aus medizinischen Gründen 11
Pflichten des Verantwortlichen für Datenschutz 12
Datenschutzbeauftragter 13

3 CYBERSECURITY DATEN- UND INFORMATIONSSICHERHEIT ... 14

Definitionen laut Verordnung (EU) 2017/745 (MDR) 15
Definitionen laut Medizinprodukte-Betreiberverordnung – MPBetreibV (nur für Deutschland) 16
Definitionen laut internationaler Standards 18
Grundsätze für IT-Sicherheit (Cybersecurity) 19
Pflichten des Verantwortlichen für IT-Sicherheit (Cybersecurity) 23
Marküberwachung der Produktsicherheit: Meldung von Security Vorkommnissen (Post-Market Surveillance) 26
Beauftragter für Medizinproduktsicherheit 28
Verantwortlicher für das Risikomanagement der vernetzten Medizintechnik (Medical-IT Risk Manager) 28
Kontaktdaten für Rückfragen über Datenschutz und Cybersecurity 28

4 STRATEGIEN UND BEWÄHRTE METHODEN 29

Datenschutz: Patienteneinwilligung 30
Datenschutz: Sicherheit der Verarbeitung (Kapitel IV, Artikel 32) 30
Anonymisierung 30
Organisatorische Maßnahmen 31

Wichtige Patientenrechte *34*
Sensible Daten *34*
Hinzufügen von Informationen und Kommentaren zu Freitextfeldern *35*
CYBERSECURITY: BENUTZERZUGRIFFSKONTROLLEN. AUTHENTISIERUNG / USER ACCESS AUTHORIZATION 35
CYBERSECURITY: BENUTZERZUGRIFFSKONTROLLEN. FERNWARTUNGSSCHNITTSTELLE 39
CYBERSECURITY: PROTOKOLLIERUNG DER NUTZER- UND SYSTEM AKTIVITÄTEN. SYSTEM-LOGS. 41
CYBERSECURITY: SICHERHEIT DER GESPEICHERTEN DATEN. DATENVERSCHLÜSSELUNG 42
CYBERSECURITY: SICHERHEIT DER DATEN AUF DEM KOMMUNIKATIONSWEG. DATENVERSCHLÜSSELUNG. AUTORISIERUNG DER NACHBARSYSTEME. 43
CYBERSECURITY: AUTHENTIFIZIERUNG DER SIDEXIS 4 KOMPONENTEN. SICHERHEITSZERTIFIKATE. 44
CYBERSECURITY: SCHUTZ GEGEN SCHADSOFTWARE UND MANIPULATION, AUTHENTIFIZIERUNG UND INTEGRITÄTSPRÜFUNG FÜR SIDEXIS 4. 44
CYBERSECURITY: AUTHENTISIERUNG DER SYSTEMKOMPONENTEN UND ABSCHALTUNG VON UNSICHEREN SCHNITTSTELLEN 47
CYBERSECURITY: DATENSICHERHEIT. VERFÜGBARKEIT DER DATEN UND DATENSICHERUNG (BACKUP) 49
CYBERSECURITY: WARTUNG VON SIDEXIS 4 (MAINTENANCE) 51
CYBERSECURITY: SICHERHEITSMANAGEMENT. ALLGEMEINES. 53

5 SYSTEM INFORMATIONEN 57

KURZER ÜBERBLICK ZU SIDEXIS 4: 58
Verwendungszweck, Indikation und Kontraindikation *58*
Freigabe *58*
Vorgesehenes Betriebsumfeld (intended operational environment of use) *58*
Systemvoraussetzungen *59*
Technischer Überblick *59*

Überblick Systemumgebung: IT-Netzwerke, Netzwerk-Zonen und sichere Kommunikationsverbindungen (Conduits)..... 68

6 RECHTLICHER HINWEIS / HAFTUNGS-AUSSCHLUSS.....71

RECHTLICHER HINWEIS / HAFTUNGSAUSSCHLUSS 72

1 Einleitung

Dieses Whitepaper beschreibt die für IT-Sicherheit, Cybersecurity und Datenschutz relevanten technischen Aspekte von Sidexis 4.

Es richtet sich hauptsächlich an diejenigen Service- und Kundenmitarbeiter, die für Installation, Konfiguration, Wartung und Benutzung verantwortlich sind. Dieses Dokument richtet sich auch an das IT-Personal, das für die Installation, Konfiguration, Wartung und Benutzung der lokalen Rechnernetze (IT-Netzwerke) zum Betreiben von Sidexis 4 zuständig ist. Weiterhin betrifft es sowohl Datenschutzbeauftragte als auch Marketing und Vertriebspersonal, die den Beschaffungsprozess begleiten.

Dieses Whitepaper zur Produktsicherheit enthält alle benötigten Informationen zu folgenden Themen:

- Beratende Hinweise dazu, wie die Anforderungen des „Allgemeinen Datenschutzes" erfüllt werden können.
- Informationen über die Maßnahmen zur IT-Sicherheit in Sidexis 4 und Hinweise zur Integration von Sidexis 4 in sichere IT-Netzwerke.
- Unterstützung beim Bewertungsprozess für Medizinprodukte.
- Informationen für generische Fragebögen.
- Informationsweitergabe an Kunden und Service-Personal.
- Sichere Installation, Konfiguration, Wartung und Betreiben des Medizinproduktes (dieses Whitepaper ersetzt weder das Installationshandbuch noch die Gebrauchsanweisung.)

Zweck des Dokuments

Die IT-Sicherheit von Medizinprodukten ist Bestandteil der Produktsicherheit und ein wichtiger Aspekt der Funktionalität. Es ist absolut notwendig eine sichere Benutzung zu gewährleisten und u. a. Folgendes sicherzustellen:

- Schutz von personenbezogenen Daten (Confidentiality)
- Integrität des Medizinproduktes, d. h. das Produkt funktioniert wie vorgesehen (Integrity)
- Verfügbarkeit des Medizinproduktes (Availability)
- Daten- und Informationssicherheit (Cybersecurity) des Medizinproduktes einschließlich der medizinischen und klinischen Daten in einer vernetzten Systemumgebung
- Weitere IT-Sicherheitsaspekte über die Datensicherheit hinaus (Nichtabstreitbarkeit / Non-Repudiation)

Um die Produktsicherheit sicherzustellen, muss ein Medizinprodukt genau gestaltet, getestet und in den Markt eingeführt werden – aber es muss auch wie beabsichtigt installiert, konfiguriert, gewartet und bedient werden. Wenn nur einer der genannten Aspekte nicht korrekt ausgeführt wird, kann die Produktsicherheit beeinträchtigt werden, was zu potenziell schweren Konsequenzen bezüglich der Unbedenklichkeit führen kann.

Datenschutz steht in engem Zusammenhang mit Produktsicherheit. Die “Datenschutzgrundverordnung“ der Europäischen Union sieht auch den Schutz von persönlichen Daten für Medizinprodukte vor.

Dieses Whitepaper dient dazu sicherzustellen, dass sowohl alle Personen und Institutionen, die für Installation, Wartung oder Bedienung eines Medizinproduktes, als auch Datenschutzbeauftragte und Verantwortliche für den Betrieb der lokalen Rechnernetze (IT-Netzwerke) alle benötigten Informationen einsehen können, um ihre Arbeit richtig auszuführen:

- Zusätzliche Informationen zu den Anforderungen der „Datenschutzgrundverordnung“ und wie das Medizinprodukt den Betreiber in der Erfüllung seiner Pflichten unterstützt
- Zusätzliche Informationen zu den Anforderungen der Europäischen Verordnung 2017/745 vom 5. April 2017 über Medizinprodukte (MDR) an die IT-Sicherheit (Cybersecurity) und wichtige Hinweise aus der Begleitdokumentation zur MDR für IT-Sicherheit *Guidance on Cybersecurity for medical devices MDCG 2019-16*
- Information zu allen produktsicherheitsrelevanten Aspekten in Bezug auf Kunden und Service-Mitarbeiter.

- Sicherstellen der Verfügbarkeit aller benötigten Daten und Richtlinien, um die sichere Installation, Konfiguration, Wartung und Benutzung vorzubereiten.

Bitte beachten Sie, dass dieses Whitepaper weder das Sidexis 4 Installationshandbuch noch das Anwenderhandbuch ersetzt. Es dient lediglich dem Zweck notwendige Informationen gebündelt und komfortabel bereitzustellen.

Zur Vermeidung von kundenindividuellen Befragungen soll das Whitepaper weiterhin alle notwendigen Informationen bereitstellen, die während des Auswahl- und Beschaffungsprozesses eines Medizinproduktes notwendig sein können.

2
Datenschutz

LAUT DER "DATENSCHUTZGRUNDVERORDNUNG" (DSGVO) DER EUROPÄISCHEN UNION

Die Datenschutzgrundverordnung der EU vom 27. April 2016, die am 25. Mai 2017 in Kraft trat (DSGVO) besagt, dass die verantwortende Person zur Einhaltung des Datenschutzgesetzes den unerlaubten Zugriff auf die ihr übermittelten oder selbst erstellten, personenbezogenen Daten Dritter (z. B. Patientendaten) verhindern muss. Als verantwortliche Person im Sinne der DSGVO gelten sowohl natürliche als auch juristische Personen (z. B. eine Firma).

Dieses Kapitel gibt einen kurzen Überblick über einige wichtige Passagen der DSGVO.

Zitierte Passagen der DSGVO sind in "*kursiv*" dargestellt.

Grundsätze für Datenschutz

Die DSGVO definiert Grundsätze darüber, inwiefern persönliche Daten erhoben oder bearbeitet werden sollen.

(Kapitel II, Artikel 5)

1. Personenbezogene Daten müssen:

> *(a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden ("Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");*
>
> *(b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden ("Zweckbindung");*
>
> *c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein ("Datenminimierung");*
>
> *d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein ("Richtigkeit");*
>
> *(e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist ("Speicherbegrenzung");*
>
> *(f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("Integrität und Vertraulichkeit");*

2. Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können ("Rechenschaftspflicht").

Datenschutz aus medizinischen Gründen

Jede Art von medizinischen Daten eine natürliche Person betreffend steht durch die DSGVO unter besonderem Schutz. Der folgende Abschnitt beschreibt die Basis auf derer diese Art von Daten bearbeitet werden darf.

Kapitel II, Artikel 9

1. *Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt,*

2. *Absatz 1 gilt nicht in folgenden Fällen:*
   ...
   (h) " die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich"

Pflichten des Verantwortlichen für Datenschutz

In einer Praxis für Zahnmedizin ist der “Verantwortliche” des Datenschutzes auch oft die juristische Person, die die Praxis besitzt – in einer Klinik kann das auch eine Gruppe von Personen sein. Es ist wichtig zu verstehen, dass der Betreiber voll verantwortlich dafür ist, alle Maßnahmen zur Einhaltung der DSGVO zu ergreifen.

Kapitel I, Artikel 4

> *„Im Sinne dieser Verordnung bezeichnet der Ausdruck:*
>
> *...*
>
> *7. Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet...”*

Kapitel IV, Artikel 24

> *1. “... Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.”*

Zu beachten ist hier, dass die DSGVO hier nicht zwischen technischen oder organisatorischen Maßnahmen zur Einhaltung des Datenschutzes unterscheidet. Tatsächlich werden technische Maßnahmen niemals vollumfänglich organisatorische Maßnahmen ersetzen können.

Datenschutzbeauftragter

Eine Praxis oder Klinik für Zahnmedizin bearbeitet immer eine große Anzahl besonderer Kategorien von persönlichen Daten zu medizinischen Zwecken. In diesem Fall müssen der Verarbeiter und Verantwortliche einen dedizierten Datenschutzbeauftragten benennen (Kapitel IV, Artikel 37, 1.(c)).

Kapitel IV, Artikel 37, 6.

Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

Aufgaben des Datenschutzbeauftragten (Kapitel IV, Artikel 39)

1. Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung …;

(b) Überwachung der Einhaltung dieser Verordnung, …sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

(c) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung…;

(d) Zusammenarbeit mit der Aufsichtsbehörde;

(e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation … und gegebenenfalls Beratung zu allen sonstigen Fragen.

3 Cybersecurity

Daten- und Informationssicherheit

LAUT DER VERORDNUNG (EU) 2017/745 (MDR) ÜBER MEDIZINPRODUKTE UND GUIDANCE ON CYBERSECURITY FOR MEDICAL DEVICES MDCG 2019-16 DER EUROPÄISCHEN UNION

Die Europäische Verordnung 2017/745 über Medizinprodukte (MDR) vom 5. April 2017, die am 25. Mai 2017 in Kraft trat, besagt, dass die Hersteller Mindestanforderungen bezüglich Eigenschaften von IT-Netzwerken und IT-Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff festlegen müssen, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind.

Dieses Kapitel gibt einen kurzen Überblick über einige wichtige Passagen der Begleitdokumentation MDCG 2019-16 für Cybersecurity zur MDR. Für den deutschen Markt werden wichtige Definitionen der Medizinprodukte-Betreiberverordnung – MPBetreibV wie der Beauftragter für Medizinproduktesicherheit erläutert.

Zitierte Passagen sind in "*kursiv*" dargestellt.

Definitionen laut Verordnung (EU) 2017/745 (MDR)

Interoperabilität

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 26)
„Interoperabilität“ bezeichnet die Fähigkeit von zwei oder mehr Produkten — einschließlich Software — desselben Herstellers oder verschiedener Hersteller,
a) Informationen auszutauschen und die ausgetauschten Informationen für die korrekte Ausführung einer konkreten Funktion ohne Änderung des Inhalts der Daten zu nutzen und/oder
b) miteinander zu kommunizieren und/oder
c) bestimmungsgemäß zusammenzuarbeiten

Bevollmächtigter

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 32)
„Bevollmächtigter“ bezeichnet jede in der Union niedergelassene natürliche oder juristische Person, die von einem außerhalb der Union ansässigen Hersteller schriftlich beauftragt wurde, in seinem Namen bestimmte Aufgaben in Erfüllung seiner aus dieser Verordnung resultierenden Verpflichtungen wahrzunehmen, und die diesen Auftrag angenommen hat

Importeur

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 33)
„Importeur“ bezeichnet jede in der Union niedergelassene natürliche oder juristische Person, die ein Produkt aus einem Drittland auf dem Unionsmarkt in Verkehr bringt

Händler

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 34)
„Händler“ bezeichnet jede natürliche oder juristische Person in der Lieferkette, die ein Produkt bis zum Zeitpunkt der Inbetriebnahme auf dem Markt bereitstellt, mit Ausnahme des Herstellers oder des Importeurs

Wirtschaftsakteur

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 35)
„Wirtschaftsakteur“ bezeichnet einen Hersteller, einen bevollmächtigten Vertreter, einen Importeur, einen Händler und die in Artikel 22 Absätze 1 und 3 genannte Person

Überwachung nach dem Inverkehrbringen

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 60)

„Überwachung nach dem Inverkehrbringen“ bezeichnet alle Tätigkeiten, die Hersteller in Zusammenarbeit mit anderen Wirtschaftsakteuren durchführen, um ein Verfahren zur proaktiven Erhebung und Überprüfung von Erfahrungen, die mit den von ihnen in Verkehr gebrachten, auf dem Markt bereitgestellten oder in Betrieb genommenen Produkten gewonnen werden, einzurichten und auf dem neuesten Stand zu halten, mit dem ein etwaiger Bedarf an unverzüglich zu ergreifenden Korrektur- oder Präventivmaßnahmen festgestellt werden kann

Vorkommnis

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 64)
„Vorkommnis“ bezeichnet eine Fehlfunktion oder Verschlechterung der Eigenschaften oder Leistung eines bereits auf dem Markt bereitgestellten Produkts, einschließlich Anwendungsfehlern aufgrund ergonomischer Merkmale, sowie eine Unzulänglichkeit der vom Hersteller bereitgestellten Informationen oder eine unerwünschte Nebenwirkung

Sicherheitskorrekturmaßnahme im Feld

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 68)
„Sicherheitskorrekturmaßnahme im Feld“ bezeichnet eine von einem Hersteller aus technischen oder medizinischen Gründen ergriffene Korrekturmaßnahme zur Verhinderung oder Verringerung des Risikos eines schwerwiegenden Vorkommnisses im Zusammenhang mit einem auf dem Markt bereitgestellten Produkt

Sicherheitsanweisung im Feld

(Kapitel I, Artikel 2 Begriffsbestimmungen, Absatz 69)
„Sicherheitsanweisung im Feld“ bezeichnet eine von einem Hersteller im Zusammenhang mit einer Sicherheitskorrekturmaßnahme im Feld an Anwender oder Kunden übermittelte Mitteilung

Definitionen laut Medizinprodukte-Betreiberverordnung – MPBetreibV (nur für Deutschland)

Tätigkeiten im Zusammenhang mit dem Betreiben und Anwenden von Medizinprodukten

(Kapitel 2 Begriffsbestimmungen, Absatz 1)
Tätigkeiten im Zusammenhang mit dem Betreiben und Anwenden von Medizinprodukten sind insbesondere
1. das Errichten,

2. das Bereithalten,
3. die Instandhaltung,
4. die Aufbereitung sowie
5. sicherheits- und messtechnische Kontrollen.

Betreiber

(Kapitel 2 Begriffsbestimmungen, Absatz 2)
Betreiber eines Medizinproduktes ist jede natürliche oder juristische Person, die für den Betrieb der Gesundheitseinrichtung verantwortlich ist, in der das Medizinprodukt durch dessen Beschäftigte betrieben oder angewendet wird. Abweichend von Satz 1 ist Betreiber eines Medizinproduktes, das im Besitz eines Angehörigen der Heilberufe oder des Heilgewerbes ist und von diesem zur Verwendung in eine Gesundheitseinrichtung mitgebracht wird, der betreffende Angehörige des Heilberufs oder des Heilgewerbes. Als Betreiber gilt auch, wer außerhalb von Gesundheitseinrichtungen in seinem Betrieb oder seiner Einrichtung oder im öffentlichen Raum Medizinprodukte zur Anwendung bereithält

Anwender

(Kapitel 2 Begriffsbestimmungen, Absatz 3)
Anwender ist, wer ein Medizinprodukt im Anwendungsbereich dieser Verordnung am Patienten einsetzt

Gesundheitseinrichtung

(Kapitel 2 Begriffsbestimmungen, Absatz 4)
Gesundheitseinrichtung im Sinne dieser Verordnung ist jede Einrichtung, Stelle oder Institution, einschließlich Rehabilitations- und Pflegeeinrichtungen, in der Medizinprodukte durch medizinisches Personal, Personen der Pflegeberufe oder sonstige dazu befugte Personen berufsmäßig betrieben oder angewendet werden

Beauftragter für Medizinproduktesicherheit

(Kapitel 6 Beauftragter für Medizinproduktesicherheit, Absätze 1 bis 4)
(1) Gesundheitseinrichtungen mit regelmäßig mehr als 20 Beschäftigten haben sicherzustellen, dass eine sachkundige und zuverlässige Person mit medizinischer, naturwissenschaftlicher, pflegerischer, pharmazeutischer oder technischer Ausbildung als Beauftragter für Medizinproduktesicherheit bestimmt ist.
(2) Der Beauftragte für Medizinproduktesicherheit nimmt als zentrale Stelle in der Gesundheitseinrichtung folgende Aufgaben für den Betreiber wahr:
1.die Aufgaben einer Kontaktperson für Behörden, Hersteller und Vertreiber im Zusammenhang mit Meldungen über Risiken von Medizinprodukten sowie bei

der Umsetzung von Sicherheitskorrekturmaßnahmen im Feld und sonstigen notwendigen Korrekturmaßnahmen,
2.die Koordinierung interner Prozesse der Gesundheitseinrichtung zur Erfüllung der Melde- und Mitwirkungspflichten der Anwender und Betreiber und
3.die Koordinierung der Umsetzung der Korrekturmaßnahmen und der Sicherheitskorrekturmaßnahmen im Feld in den Gesundheitseinrichtungen.
(3) Der Beauftragte für Medizinproduktesicherheit darf bei der Erfüllung der nach Absatz 2 übertragenen Aufgaben nicht behindert und wegen der Erfüllung der Aufgaben nicht benachteiligt werden.
(4) Die Gesundheitseinrichtung hat sicherzustellen, dass eine Funktions-E-Mail-Adresse des Beauftragten für die Medizinproduktesicherheit auf ihrer Internetseite bekannt gemacht ist.

Definitionen laut internationaler Standards

(ISO/TR 24971:2020-06 Medical devices - Guidance on the application of ISO 14971, Medizinprodukte - Leitfaden für die Anwendung von ISO 14971)

Security

"Security": a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences, where hostile acts or influences cloud be intention.
Security as defined above includes cybersecurity and data and systems security.

Confidentiality / Vertraulichkeit der Daten/des Systems

"Confidentiality": property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
(Erläuterung aus der Norm ISO/TR 24971:2020, Anhang F)
In the instances, loss of confidentiality could be more important, because disclosure of personal health information can create a potential for blackmail.

Integrity / Integrität der Daten/des Systems

"Integrity": property of accuracy and completeness.
(Erläuterung aus der Norm ISO/TR 24971:2020, Anhang F)
Loss of integrity could result in changes to a patient´s medical record (e. g. changes in drug orders or medical data/images)

Availability / Verfügbarkeit der Daten/des Systems
"Availability": property of being accessible and usable upon demand by and authorized entity.
(Erläuterung aus der Norm ISO/TR 24971:2020, Anhang F)
Loss of availability of the medical device can result in delay of diagnosis or delay of treatment.

Grundsätze für IT-Sicherheit (Cybersecurity)

Die Verordnung (EU) 2017/745 (MDR) einschließlich der Begleitdokumentation für Cybersecurity MDCG 2019-16 definiert Grundsätze darüber, inwiefern Daten- und Informationssicherheit (Cybersecurity) für Medizinprodukte einschließlich Medical Device Software (MDSW) berücksichtigt werden sollen.

Weitere ergänzenden Grundsätze werden von nationalen gesetzlichen Auflagen wie z.B. Medizinprodukte-Betreiberverordnung – MPBetreibV (Deutschland) definiert aber auch von internationalen Normen wie z.B. ISO/TR 24971 u.a.

Welcher Zusammenhang gibt es zwischen einem Medizinprodukt und den IT-Sicherheitsmaßnahmen?

Eine vollständige Antwort geht über Rahmen dieses Dokumentes hinaus, aber es wird in kurzer Form hier beantwortet.

Die Definition von IT-Sicherheitsmaßnahmen für ein bestimmtes Betriebsumfeld (*intended environment / intended operational environment of use)* eines Medizinproduktes dient dazu, die aus Daten- und Informationssicherheit resultierenden Risiken für das Medizinprodukt in einem konkreten Betriebsumfeld zu mindern und im besten Fall zu beseitigen, welche den bestimmungsgemäßen Einsatz der Software hindern sollen und damit auch die Leistungserbringung von wesentlichen funktionalen Merkmalen des Medizinproduktes (intended use).

Dies ist in der Verordnung (EU) 2017/745 (MDR) kurz beschrieben wie folgt:

(Verordnung (EU) 2017/745 (MDR), Anhang I, Kapitel II, Absatz 17.4)
Die Hersteller legen Mindestanforderungen bezüglich Hardware, Eigenschaften von IT-Netzen und IT-Sicherheitsmaßnahmen einschließlich des Schutzes vor

unbefugtem Zugriff fest, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind

(Verordnung (EU) 2017/745 (MDR), Anhang I, Kapitel III, Absatz 23.4, Buchstabe ab)
bei Produkten, zu deren Bestandteilen programmierbare Elektroniksysteme, einschließlich Software, gehören, oder Produkte in Form einer Software enthalten, Mindestanforderungen bezüglich Hardware, Eigenschaften von IT-Netzen und IT-Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind

Des Weiteren weist die zur MDR Begleitdokumentation *MDCG 2019-16 Guidance on Cybersecurity for medical devices* auf eine notwendige Zusammenarbeit der verschiedenen Wirtschafts- (siehe MDR Definitionen oben) und technischen Akteure (Siehe Begleitdokumentation MDCG 2019-16, Kapitel 2, Absatz 6 Joint Responsibility – Integrator-Operator-Users) hin.

Welche spezifischen Sicherheitsmaßnahmen sind für vernetzte Medizinprodukte zu erwarten?

Für die Anforderungen an die Produktsicherheit hinsichtlich der Daten- und Informationssicherheit, wurde die Begleitdokumentation zu der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 *Guidance on Cybersecurity for medical devices MDCG 2019-16* von der Koordinierungsgruppe Medizinprodukte (Medical Device Coordination Group MDCG) berücksichtigt.

Sidexis 4 verfügt bereits über Risikomaßnahmen für die Daten- und Informationssicherheit (Cybersecurity) einschließlich mancher Maßnahmen für eine sichere Anwendung von Sidexis 4 in einem vernetzten Betriebsumfeld (IT-Netzwerke), wie folgt (nicht-abschließend):

- Empfehlungen für ein sicheres Betriebsumfeld (Microsoft Windows): Automatisches Ausloggen, Verwaltung von Nutzerkonten, Sicherheitsupdates u.a.
- Authentisierung, Authentifizierung und Autorisierung von Sidexis 4 Komponenten
- System-Logs
- Management von Sicherheitsupdates für Sidexis und Betriebssystem

- Anonymisierung von Personendaten
- Support für Verschlüsselung von Patientendaten durch Software Dritter (z.B. Microsoft Windows Bitlocker)
- Sperrung (Abschaltung) von unsicheren Systemschnittstellen
- Prüfung der Software-Integrität
- Authentisierung und Autorisierung von Systemkomponenten und Schnittstellen (Knoten/Nachbarsysteme)
- Überwachung der Fernwartungszugänge
- Begleitdokumentation für den Datenschutz und die Produktsicherheit (dieses Dokument)

(Guidance on Cybersecurity for medical devices MDCG 2019-16, Kapitel 3, Absatz 3)
Security capabilities may be determined as suitable risk-control measures. The design and implementation of such capabilities need to comply with the state of the art (see Annex I, sections 17.2 (MDR) or 1, 4, 16.2 (IVDR)) and cover a wide range of technical areas (see Table 3).

Table 3: Indicative list of security Capabilities for MD
Automatic Logoff
Audit Controls
Authorization
Configuration of Security Features
Cybersecurity Product Upgrades
Personal Data De-Identification
Data Backup and Disaster Recovery
Emergency Access
Personal Data Integrity and Authenticity
Malware Detection / Protection
Node Authentication
Person Authentication
Physical Locks
System and OS Hardening
Security and Privacy Guides
Personal Data Storage Confidentiality
Transmission Confidentiality
Transmission Integrity

Nähere Informationen über die Risikomaßnahmen für Cybersecurity *by Design* in Sidexis 4 finden Sie in den Kapiteln *Strategien und bewährte Methoden* und *System Informationen.*

Neben der Sicherheitsmaßnahmen *by Design*, welche anderen Sicherheitsmaßnahmen müsste man für Cybersecurity noch berücksichtigen?

Neben den Anforderungen an die Daten- und Informationssicherheit *by Design,* wie z.B. eine Authentisierung der Kommunikation zwischen dem Sidexis Client und dem Sidexis Server, existieren weitere Anforderungen an die IT-Sicherheit, die außerhalb des Produktumfangs von Sidexis 4 sind, und somit auch außer der Verantwortung von Dentsply Sirona - SIRONA Dental Systems GmbH im nachfolgenden als Hersteller bezeichnet, wie z.B. die Vertraulichkeit und Integrität der Datenübertragung in den lokalen Rechnernetzen des Betriebes.

Hierfür entstehen auch Anforderungen für sämtliche Wirtschaftsakteure (Bevollmächtigte, Importeure, Händler) im Sinne von der Verordnung (EU) 2017/745 aber auch im Rahmen der deutschen Medizinprodukte-Betreiberverordnung – MPBetreibV (Anwender, Betreiber, Gesundheitseinrichtung, Beauftragter für Medizinproduktesicherheit), wie im nachfolgenden Absatz *Pflichten des Verantwortlichen* zu entnehmen sind.

Siehe Beispiele für die Konfiguration eines lokalen Rechnernetzes (IT-Netzwerk) im Kapitel *Überblick Systemumgebung: IT-Netzwerke, Netzwerk-Zonen und sichere Kommunikationsverbindungen (Conduits)*.

Neben den technischen Maßnahmen sind auch organisatorische Maßnahmen für die Daten- und Informationssicherheit (Cybersecurity) nötig wie z.B. eine beidseitige Kommunikation zwischen Betreiber und Hersteller zur Klärung eines Vorkommnisses für Cybersecurity und zur gemeinsamen Definition einer Sicherheitskorrekturmaßnahme im Feld (siehe Definition im Absatz *Definitionen laut (EU) Verordnung 2017/745 (MDR)* oben).

Für eine erfolgreiche und sichere Integration von Sidexis 4 in die vorgesehene Produktumgebung (intended environment) müssen sämtliche Akteure, wie oben in den Kapiteln *Definitionen laut (EU) Verordnung 2017/745 (MDR) und Medizinprodukte-Betreiberverordnung – MPBetreibV,* koordiniert zusammenarbeiten und agieren.

Pflichten des Verantwortlichen für IT-Sicherheit (Cybersecurity)

Für die Daten- und Informationssicherheit (Cybersecurity) verteilt sich die Verantwortung auf mehrere Akteure und Rollen, die für die Erfüllung der Anforderungen an die Cybersecurity verantwortlich sind, wie von der Gesetzgebung und der Normung (Industrie Best-Practices) definiert.

I. Akteure und Pflichten aus der Verordnung (EU) 2017/745 MDR:
   a. Der Hersteller wird die Anforderungen an die Daten- und die Informationssicherheit (Cybersecurity) von der Entwicklung des Medizinproduktes und über den gesamten Produktlebenszyklus berücksichtigen.
   Das Risikomanagementprozess wird sowohl für die Risiken für die Patientensicherheit (Safety), für den Patientendatenschutz (Privacy) als auch für die Daten- und Informationssicherheit (Cybersecurity) angewandt, wie vom harmonisierten Standard für Risikomanagement der Medizinprodukte (*ISO14971:2019 Medical devices — Application of risk management to medical devices*) und der Begleitdokumentation MDCG 2019-16 zur *Verordnung (EU) 2017/745 (MDR)* für Cybersecurity empfohlen wird.
   b. Importeure
   (Artikel 13 Allgemeine Pflichten der Importeure, Absatz 8) Importeure, denen Beschwerden und Berichte seitens Angehöriger der Gesundheitsberufe, der Patienten oder Anwender über mutmaßliche Vorkommnisse im Zusammenhang mit einem Produkt, das sie in den Verkehr gebracht haben, zugehen, leiten diese unverzüglich an den Hersteller und seinen Bevollmächtigten weiter.
   c. Händler
   (Artikel 14 Allgemeine Pflichten der Händler, Absatz 5) Händler, denen Beschwerden und Berichte seitens Angehöriger der Gesundheitsberufe, der Patienten oder Anwender über mutmaßliche Vorkommnisse im Zusammenhang mit einem Produkt, das sie bereitgestellt haben, zugehen, leiten diese unverzüglich an den Hersteller und gegebenenfalls den Bevollmächtigten des Herstellers und den Importeur weiter. Sie führen ein Register der Beschwerden, der nichtkonformen Produkte und der Rückrufe und Rücknahmen, und sie halten den Hersteller und gegebenenfalls dessen Bevollmächtigten und den Importeur

über diese Überwachungsmaßnahme auf dem Laufenden und stellen ihnen auf deren Ersuchen alle Informationen zur Verfügung.

Für Importeure und Händler ist die Bereitstellung von Informationen über mutmaßliche Vorkommnisse (Patientensicherheit einschließlich Cybersecurity) für Sidexis 4 einschließlich seiner Systemumgebung (*intended environment*) dem Hersteller verpflichtend, damit der Hersteller seine Pflichten zur Überwachung und Meldung von Vorkommnissen auf dem Markt für Sidexis 4 nachkommen kann.

II. Akteure und Pflichten aus der Medizinprodukte-Betreiberverordnung -MPBetreibV:
    a. Sämtliche Akteure und Rollen (Anwender, Betreiber, Gesundheitseinrichtung, Beauftragter für Medizinproduktesicherheit) als von der Verordnung definiert tragen zur Erfüllung der Sicherheitsanforderungen (Maßnahmen für Patientensicherheit einschließlich Cybersecurity) bei. Siehe Absatz *Definitionen laut Medizinprodukte-Betreiberverordnung – MPBetreibV (nur für Deutschland)* oben für nähere Informationen.
    b. Überwachung des Betriebsumfelds für verbundene Medizinprodukte und Meldung von Vorkommnissen an den Hersteller
    (Kapitel 4 Allgemeine Anforderungen, Absatz 4) Miteinander verbundene Medizinprodukte sowie mit Zubehör einschließlich Software oder mit anderen Gegenständen verbundene Medizinprodukte dürfen nur betrieben und angewendet werden, wenn sie zur Anwendung in dieser Kombination unter Berücksichtigung der Zweckbestimmung und der Sicherheit der Patienten, Anwender, Beschäftigten oder Dritten geeignet sind.

    Das Betriebsumfeld schließt die lokalen Rechnernetze (IT-Netzwerke) ein und wird als *intended operational environment of use* in der Begleitdokumentation MDCG 2019-16 zur *Verordnung 2017/745 (MDR)* für Cybersecurity bezeichnet.
    c. Das ordnungsgemäße Anwenden von Sidexis 4 als Medizinprodukt einschließlich der sicheren und interoperablen Anwendung von den betrieblichen IT-Netzwerken obliegt der Betreiberverantwortung (siehe Definition von *Interoperabilität*

im Absatz *Definitionen laut Verordnung (EU) 2017/745 (MDR*).

(Kapitel 3 Pflichten des Betreibers, Absatz 1)
Der Betreiber hat die ihm nach dieser Verordnung obliegenden Pflichten wahrzunehmen, um ein sicheres und ordnungsgemäßes Anwenden der in seiner Gesundheitseinrichtung am Patienten eingesetzten Medizinprodukte zu gewährleisten.

d. Der Hersteller empfiehlt stets dem Betreiber die Benennung eines Beauftragten für Medizinproduktesicherheit, auch wenn diese Rolle bei Gesundheitseinrichtungen mit weniger als 20 Beschäftigen nicht verpflichtend ist.
(Kapitel 6, Sicherheitsbeauftrager für Medinproduktesicherheit). Siehe Definition und Pflichten im Absatz *Definitionen laut Medizinprodukte-Betreiberverordnung – MPBetreibV* oben

e. Für Sidexis 4 und die damit verbundenen Systeme zur Diagnose mit bildgebenden Verfahren muss der Betreiber ein Medizinproduktebuch führen und die Angaben zur Vorkommnissen für Patientensicherheit einschließlich Cybersecurity darin zu protokollieren.

(Kapitel 12 Medizinproduktebuch, Absatz 1)
Für die in den Anlagen 1 und 2 aufgeführten Medizinprodukte hat der Betreiber ein Medizinproduktebuch nach Absatz 2 zu führen.

(Kapitel 12 Medizinproduktebuch, Absatz 2, Ziffer 6)
In das Medizinproduktebuch, für das alle Datenträger zulässig sind, sind folgende Angaben zu dem jeweiligen Medizinprodukt einzutragen:
(6) Angaben zu Vorkommnis Meldungen an Behörden und Hersteller.

III. Akteure und Pflichten aus der internationalen Normung und Industrie Best-Practices für die Daten- und Informationssicherheit (Cybersecurity):

Wie bereits erwähnt schließt die Überwachung des Betriebsumfeldes durch den Betreiber die lokalen Rechnernetze (IT-Netzwerke) ein. Auch wenn die Anwendung des internationalen Standards *IEC 80001-1:2021* nicht verpflichtend ist, ist es sinnvoll, dass Sie als Betreiber

Prozesse für das Risikomanagement der Daten- und Informationssicherheitsrisiken festlegen, die aus der Integration von Sidexis 4 in Ihre betriebliche Rechnernetze (IT-Netzwerke) resultieren.

Für die Anwendung des Risikomanagements für die IT-Netzwerke des Betreibers wird dem Betreiber empfohlen einem Verantwortlichen dafür zu nennen. Hierfür definiert der Standard *IEC 80001-1:2021 die Rolle des Medical IT Risk Managers,* der sämtliche Aufgaben für die Einhaltung der Daten- und Informationssicherheit für die verbundenen Medizinprodukte wie Sidexis 4 in der Betreiberorganisation übernehmen könnte.

Der *Medical-IT Risk Manager* muss zusammen mit dem *Beauftragten für Medizinproduktsicherheit* (siehe Definition oben im Absatz *Definitionen laut Medizinprodukte-Betreiberverordnung – MPBetreibV)* an der Überwachung potenzieller Cybersecurity Risiken im Betriebsumfeld, an der Meldung von Vorkommnissen und an der Umsetzung von Sicherheitskorrekturmaßnahmen.

(*IEC 80001-1:2021 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software — Part 1: Application of risk management)*

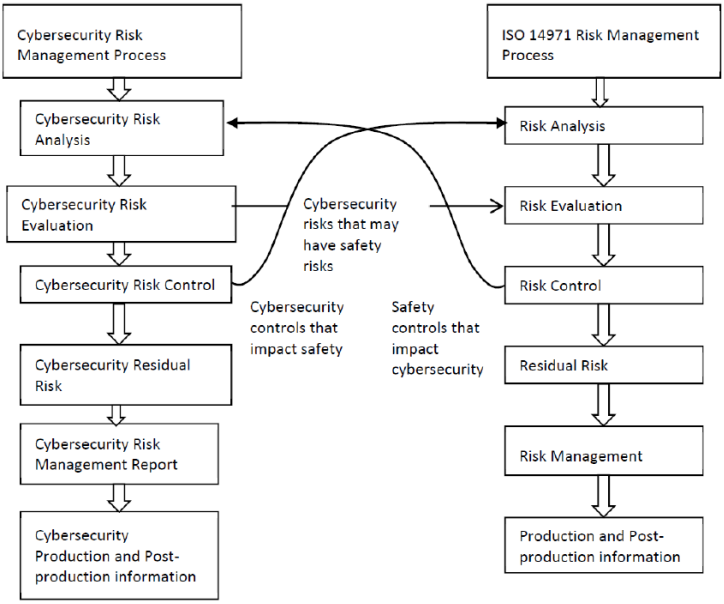
Marküberwachung der Produktsicherheit: Meldung von Security Vorkommnissen (Post-Market Surveillance)

Wie bereits erwähnt sind die Risiken aus der Daten- und Informationssicherheit (Cybersecurity) für Medizingeräte, einschließlich Software als Medical Device, wie die Risiken für die Patientensicherheit (Safety) gemäß ISO14971 zu handhaben.

Die Cybersecurity Risiken für Sidexis 4 werden vom Risikomanagementprozess für Sidexis 4 kontinuierlich überwacht und somit in

den Risikomanagementplan und die Risikoakte (Risk Management File) integriert.

Die Überwachung der Cybersecurity Risiken und ihre Bewertung hinsichtlich ihrer potenziellen Auswirkung auf die Patientensicherheit findet über den gesamten Produktlebenszyklus statt in Anlehnung an die Empfehlung MDCG 2019-16 der Koordinierungsgruppe (Medical Device Coordination Group MDCG) zur MDR.



Quelle: MDCG 2019-16 Guidance on Cybersecurity for medical devices, MDCG 2019-16, December 2019, Annex IV – Cybersecurity risk management process and safety risk management relationship.

Zur Überwachung der Cybersecurity Vorkommnisse (Security Incidents/ Vulnerabilities) sind zusammen mit dem Hersteller auch sämtliche Wirtschaftsakteure (Betreiber, Händler, Importeure) im Rahmen ihrer Geschäftsprozesse für Post-Market Surveillance und Security Incident Management verpflichtet.

Nützliche Informationsquellen für Security Vorkommnisse (Incidents) neben den branchenspezifischen Datenbanken sind die nationalen *Computer*

Emergency Response Teams (CERT) wie z.B. CERT Germany https://www.cert-bund.de und CERT European Union https://cert.europa.eu.

Beauftragter für Medizinproduktsicherheit

Siehe Definition im Kapitel *Definitionen laut Medizinprodukte-Betreiberverordnung – MPBetreibV (nur für Deutschland)*

Verantwortlicher für das Risikomanagement der vernetzten Medizintechnik (Medical-IT Risk Manager)

Siehe Definition im Kapitel *Pflichten des Verantwortlichen für IT-Sicherheit (Cybersecurity)*

Kontaktdaten für Rückfragen über Datenschutz und Cybersecurity

Kontaktieren Sie in Ihrer Organisation zuerst:

- Ihren Beauftragten für Datenschutz oder
- Ihren Beauftragten für Medizinproduktsicherheit oder
- Ihren Verantwortlichen in Fragen Daten- und Informationssicherheit (Cybersecurity) bzw. Ihren Medical-IT Risikomanager

um Ihre Rückfrage schnellstmöglich beantworten zu können.

Alternativ erreichen Sie uns auch über unser Kontaktformular online: https://siroforcemobile.dentsplysirona.com

4 Strategien und bewährte Methoden

FÜR DATENSCHUTZ, DATEN- UND INFORMATIONSSICHERHEIT (CYBERSECURITY)

Dieses Kapitel gibt Ihnen Hinweise zu bewährten Methoden für organisatorische und technische Maßnahmen und zeigt auf, wie Sidexis 4 Sie in Sachen Datenschutz und IT-Sicherheit (Cybersecurity) unterstützen kann.

Datenschutz: Patienteneinwilligung

Rechtlich gesehen ist es am sichersten, personenbezogene Daten erst nach Patienteneinwilligung zu verarbeiten. Die DSGVO definiert einige Regeln, wie diese Einwilligung einzuholen ist.

(Kapitel II, Artikel 7,8)

- *Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.*
- *…die Einwilligung…muss… in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von … anderen Sachverhalten klar zu unterscheiden ist.*
- *Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. … Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.*
- *…hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. … Die Mitgliedstaaten können durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf.*

Datenschutz: Sicherheit der Verarbeitung (Kapitel IV, Artikel 32)

(Kapitel IV, Artikel 32)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;

Anonymisierung

- Anonymisieren Sie den angemeldeten Patienten in Sidexis 4, indem Sie über die Einstellungen nur die Karteinummer des Patienten im linken oberen Bildschirmrand anzeigen lassen.
- Anonymisieren Sie Patientendaten bei DICOM Exporten (Medien ohne Patienteninformationen) aus Sidexis 4, um diese mit anderen Zahnmedizinern aus einer anderen rechtlichen Einheit (z.B. einer anderen Praxis) zu teilen → Nutzen Sie hierzu bevorzugt den DICOM Export ausschließlich auf einen verschlüsselten Datenträger, wenn keine Anonymisierung der Daten möglich oder gewünscht ist.
- Sidexis 4 erlaubt Ihnen auch einen Ausdruck der Patientendaten ohne Patienteninformationen mit der Funktion *Ausdruck anonymisieren.*

Organisatorische Maßnahmen

- Definieren Sie Verhaltensrichtlinien bezüglich des Datenschutzes in der entsprechenden zahnmedizinischen Praxis
- Prüfen Sie Ihre Pflichten für Daten- und Informationssicherheit (Cybersecurity), insbesondere den potenziellen Bedarf eines *Beauftragten für Medizinproduktesicherheit* und/oder eines *Medical-IT Risikomanagers*. Siehe Kapitel *Pflichten des Verantwortlichen (Cybersecurity)* oben.
- Erstellen Sie eine Leitlinie zur Informationssicherheit
- Definieren Sie Zugriffsrichtlinien mit Protokollierung der Personenkreise und die damit verbundenen Rollen für Ihre eigenen Mitarbeiter und ggfs. die Mitarbeiter Ihres externen IT-Geschäftspartners, die an der Definition und/oder Umsetzung von den Eigenschaften Ihrer IT-Netze und IT-Sicherheitsmaßnahmen z.B. Schutz vor unbefugtem Zugriff lokal vor Ort oder mit Fernzugriff (remote) teilnehmen.
- Qualifizieren Sie Ihr Praxispersonal zur Ausführung der Verhaltensrichtlinien für Datenschutz und für Cybersecurity
  - Bewahren Sie eine Kopie jedes Trainings für Ihre Angestellten auf.
  - Wählen Sie nur qualifiziertes Personal zur Verarbeitung von personenbezogenen Daten und von IT-Infrastruktur einschl. Cybersecurity-Themen aus (bezüglich Expertise und Zuverlässigkeit)
  - Mitarbeiter, die in der Verarbeitung von personenbezogenen Daten involviert sind, sollten sich in einer Festanstellung befinden (vertragsgebunden)

- Dokumentieren Sie die Verarbeitungsprozesse in Ihrer Praxis

(Kapitel IV, Artikel 30)

1. Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

(g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

2. Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, …

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(Begleitdokumentation für Cybersecurity zur Verordnung (EU)2017/745 (MDR), MDCG 2019-16 Guidance on Cybersecurity for medical devices)

Wichtige Patientenrechte

Es existieren einige zusätzliche Patientenrechte bezüglich des Umgangs mit ihren persönlichen Daten:

- *Recht auf Löschung ('Recht auf Vergessenwerden') (Kapitel III, Artikel 17)*

  Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, …

  - Sidexis 4 unterstützt das Löschen von personenbezogenen Daten ab der Version Sidexis 4 V4.3
  - Vorsicht: Das Recht auf Löschung überstimmt nicht die nationalen Richtlinien zur Aufbewahrung von Röntgenaufnahmen

- *Recht auf Datenübertragbarkeit (Kapitel III, Artikel 20)*

  Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, …

  - Sidexis 4 ermöglicht den Export von personenbezogenen Daten in standardisierten Formaten (z. B. DICOM)

- *Widerspruchsrecht (Kapitel III, Artikel 21)*

  Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, … Widerspruch einzulegen

  - Vorsicht: Das Widerspruchsrecht überstimmt nicht die nationalen Richtlinien zur Aufbewahrung von Röntgenaufnahmen

Sensible Daten

- Sidexis 4 verarbeitet persönliche Daten von Patienten laut der (EU) Datenschutzgrundverordnung. Dazu gehören:
  - Name
  - Geburtsdatum
  - Karteinummer. Aus Datenschutzgründen empfehlen wir Ihnen, keine Kranken- oder Sozialversicherungsnummer hier einzutragen.
  - Foto des Patienten
  - Röntgenaufnahmen und 3D Volumina
  - Intraorale Fotos
  - Diagnostische Befunde und therapeutische Informationen
  - (Sozial-)Versicherungsnummer
- Medien können beim Export anonymisiert werden.
- Sidexis 4 kann so konfiguriert werden, dass keine persönlichen Patientendaten angezeigt werden. Ausgenommen hiervon ist die Karteinummer, die zwingend benötigt wird, um den Patienten identifizieren zu können.

Hinzufügen von Informationen und Kommentaren zu Freitextfeldern

Freitextfelder oder Kommentarfelder werden verwendet, um Nutzern zu ermöglichen, etwas mit eigenen Worten zu beschreiben. Einträge sollten neutral und sachlich sein.

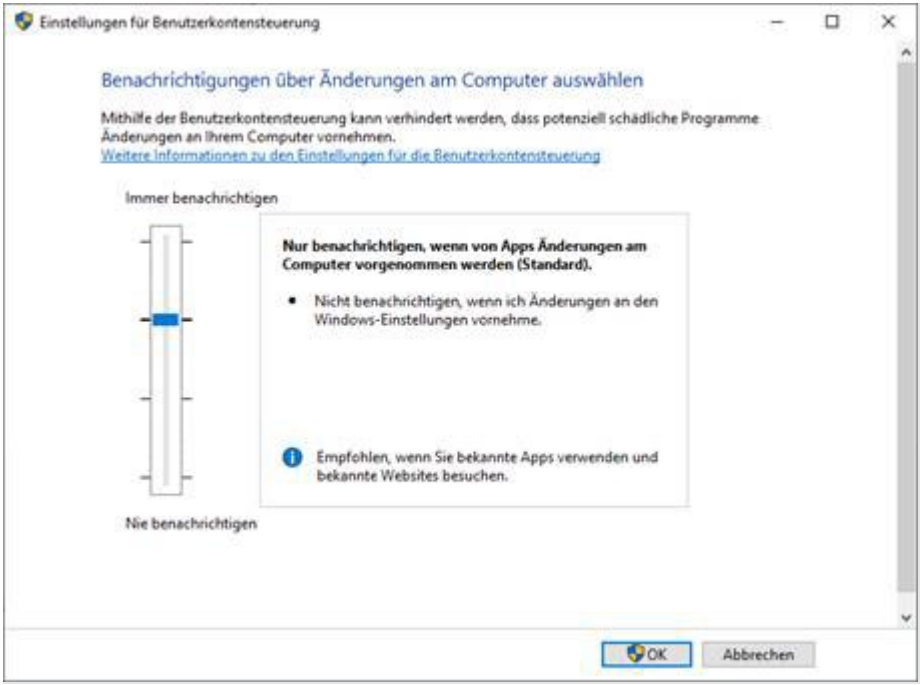
Bitte verwenden Sie diese Freitextfelder und Kommentarfelder nicht, um persönliche, Patienten- oder Gesundheits- Daten wie z. B. den Namen des Patienten hinzuzufügen.

Cybersecurity: Benutzerzugriffskontrollen. Authentisierung / User Access Authorization

Sidexis 4 verwendet Sicherheitsmaßnahmen gegen einen unbefugten Zugriff auf das System und Daten. Der vorhandene Benutzerzugriffskontrollmechanismus Ihres Betriebssystems (Microsoft Windows) ermöglicht eine beschränkte Vergabe von Privilegien zur Durchführung bestimmter Operationen z.B. Zugriff auf die Datenbank.

Mithilfe der Windows Benutzerkontensteuerung (UAC) kann verhindert werden, dass potenziell schädliche Programme Änderungen an Ihrem Computer vornehmen.

Stellen Sie die Benutzerkontensteuerung (UAC) auf jeder Windows Arbeitsstation mindestens auf Stufe 3 ein, diese ist in Windows standardmäßig ausgewählt: „Nur benachrichtigen, wenn von Apps Änderungen am Computer vorgenommen werden (Standard).“



Limitieren Sie den Zugang zu dem Sidexis 4 Server und zu den Arbeitsstationen soweit möglich:

- Nur System-Administratoren (Microsoft Windows) sollten Zugang zum Server haben
- Definieren Sie eine strikte Passwortrichtlinie zur Definition sicherer Passwörter hinsichtlich der Länge, der Nutzung von Sonderzeichen

und der Frequenz zur Änderung der Passwörter und wenden Sie sie für jedes eingerichtete Benutzerkonto auf Ihrem Betriebssystem (Microsoft Windows) an, das Sidexis 4verwenden soll. Eine mehrfache Nutzung von Sidexis 4 an einer Arbeitsstation durch mehrere Anmeldungen an derselben Arbeitsstation wird unterbunden.

- Sperren Sie die Arbeitsstation, sobald Sie Ihre Arbeitsstation nicht mehr benötigen. Nutzen Sie dafür die Funktionen Ihres Betriebssystems (Microsoft Windows) wie die automatische Bildschirmsperre nach einer bestimmten Zeit. Unterweisen Sie alle Nutzer in das sichere Verlassen ihrer Arbeitsplätze.

Für die Installation von Sidexis 4 ist ein Administrator-Nutzerkonto in Ihrem Betriebssystem (Microsoft Windows) erforderlich.

Das Installationsprogramm (Setup) von Sidexis 4 legt einen Benutzer ohne Administrationsrechte für den Sidexis 4 Server an. Dieser Benutzer (Sidexis4Service) ist zum Starten des Sidexis 4 Server Dienstes, zur Durchführung der Datenbank-Backups sowie für den Zugriff (auch durch Service-Techniker) auf den geschützten Datenbereich SECURE MEDIA SHARE (PDATASEC) vorgesehen.

Sidexis 4 erfordert eine Authentisierung durch die Eingabe eines Passworts bzw. eine zertifikatsbasierte Authentifizierung für folgende Abläufe:

- Zugriff auf kritische Funktionen oder geschützte Einstellungen in der Bedienungsoberfläche
- Kommunikationsfähigkeit zwischen Sidexis Client und Sidexis Server
- Durchführung von Operationen auf Sidexis Datenbanken

Im Rahmen der Erstinstallation bzw. Update von Sidexis 4 ist die Vergabe der folgenden benutzerspezifischen Passwörter erforderlich:

- SQL SA Passwort: Passwort für den Service Administrator der Sidexis SQL-Datenbank Instanz
- Sidexis 4 Service (Sidexis4Service) Passwort: Passwort für den Windows-Benutzer "Sidexis 4Service" des Sidexis 4 Services (Servers) und MEDIA SHARES (PDATA und PDATASEC)
- Sidexis 4 Admin (S4Admin) Passwort: Passwort für Admin-Benutzer im Sidexis 4 für den Zugriff auf geschützte Einstellungen und

sensiblen Funktionen (wie z.B. Medien verschieben oder Patient löschen) von Sidexis 4

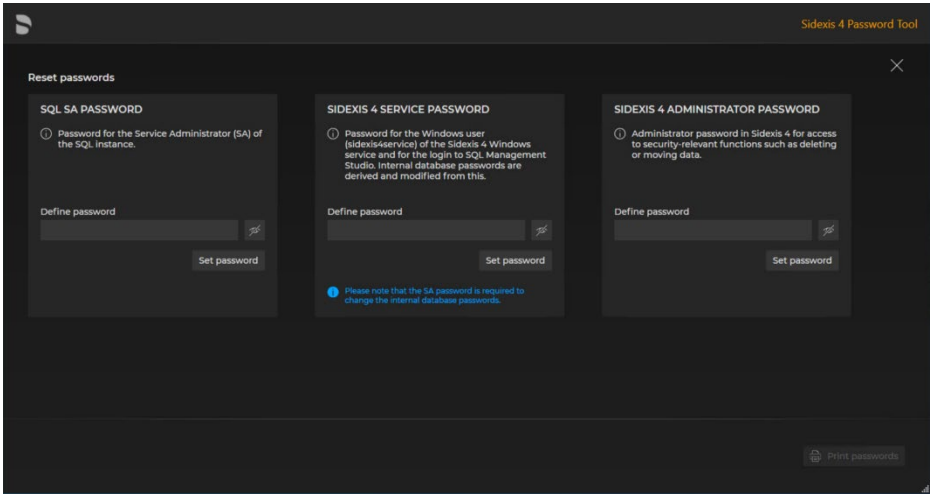
Während des Betriebs empfehlen wir das Ändern der Passwörter in regelmäßigen Zeitabständen.

Sidexis 4 verfügt hierfür über ein eigenständiges Passwort-Tool, welches Sie zum Setzen und Ändern von sicheren Passwörtern unter Verwendung der Sicherheitsrichtlinie für Passwörter verwenden können. Die Ausführung vom Passwort-Tool setzt einen Windows-Benutzer mit Administrator-Rechten voraus und kann nur auf dem Computer benutzt werden, worauf der Sidexis 4 Server installiert wurde. Das Passwort-Tool stellt die Integrität der definierten Passwörter mit Hilfe von kryptographischen Funktionen sicher.

Das Tool ist verfügbar in den Sprachen Deutsch (DE), Englisch (EN), Italienisch (IT), Französisch (FR) und Spanisch (ES). Das Tool verwendet die ausgewählte Sprache in Ihrem Windows-Rechner und Englisch als Standardeinstellung.

Sie finden das Passwort Tool (Dateinamen: PasswordTool.exe) sowohl auf dem Installationsverzeichnis Ihrer Sidexis Server-Installation als auch im Windows Startmenü unter dem Verzeichnis SIRONA neben der Sidexis 4 Software.

Weitere Informationen über das Passwort-Tool finden Sie im Installationshandbuch von Sidexis 4.

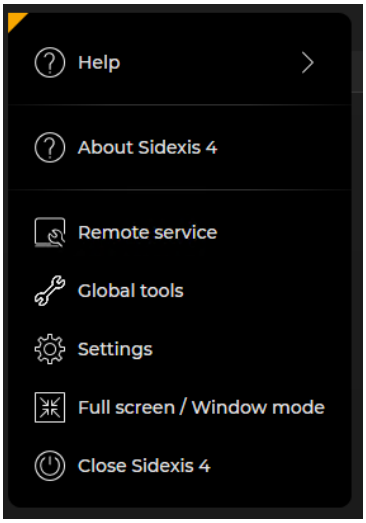


Cybersecurity: Benutzerzugriffskontrollen. Fernwartungsschnittstelle

Für den Kundenservice bei technischen Fragen und für die Fernwartung von Sidexis 4 wird das Softwareprodukt *Teamviewer* verwendet. Dieses Produkt ist kein Bestandteil von Sidexis 4.

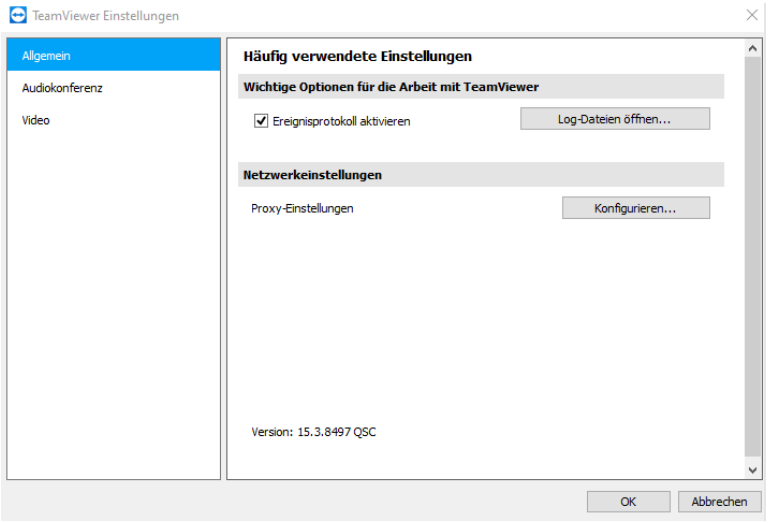
Auf der Bedienungsoberfläche von Sidexis 4 im Hauptmenü „Sidexis 4 Remote Service“ finden Sie den Support zur Fernwartung (Remote Support Link) zum Download des Teamviewer-Clients. Nach Ihrer lokalen Freigabe öffnet sich der Weblink https://get.teamviewer.com/ds_imaging_support und die Teamviewer Software wird auf Ihren Rechner heruntergeladen.

Sie finden die wichtigsten Informationen über Ihre Sidexis 4 Installation auf der Bedienungsoberfläche im Menü *Anzeige Programminfo* unter der Rubrik *Remote Service*.



Teamviewer erfasst alle Aktivitäten der Sitzung und die Aktionen der Verwaltungskonsole in einem integrierten Berichtsprotokoll. Der Zugriff auf die Teamviewer Aufzeichnungen und Berichtsprotokollen (Audit Log) erfolgt nur für autorisierte Benutzer gemäß einer Benutzerrichtlinie.

Prüfen Sie regelmäßig die Fernwartung -Logdatei (Berichtprotokoll Teamviewer_Logfile), um Ihre Freigaben auf Ihrer Arbeitsstation für den Fernzugriff und potenziell nicht autorisierte Fernzugriffe zu erkennen.



Nähere Informationen dazu finden Sie im Servicehandbuch von Sidexis 4.

Cybersecurity: Protokollierung der Nutzer- und System Aktivitäten. System-Logs.

Die Sidexis System-Logdateien mit sensiblen Daten (DBMigration, Löschen, Verschieben) werden in dem gesicherten Datenbereich SECURE MEDIA SHARE (PDATASEC) unter dem Pfad <PDATASEC>\Log\Sidexis4 gespeichert. Reguläre Sidexis System-Logdateien ohne sensible Daten werden unter folgendem Pfad gespeichert: %PROGRAMDATA%\Sirona\Log\Sidexis4.

Detaillierte Informationen über Logdateien und derer Speicherort sowie deren Inhalt erhalten Sie im Glossar des Service-Handbuchs.

Desgleichen empfehlen wir Ihnen auch die regelmäßige Nachprüfung der Sidexis **Datenbank-Logdateien** (SQL-Server Errorlog-Dateien), um potenzielle verdächtige Datenbankzugriffe frühzeitig zu identifizieren.

Die **Datenbank-Logdateien** (SQL-Server Errorlog-Dateien) finden Sie unter dem Installationsverzeichnis auf:
“%ProgramFiles%/Microsoft SQL Server\MSSQL14.SIDEXIS_SQL\Log”

Prüfen Sie zusätzlich regelmäßig auch die Windows Benutzer-Logdatei, um potenzielle verdächtige Zugänge auf Ihr System zu erkennen.

Prüfen Sie regelmäßig die **Fernwartung -Logdatei** (Berichtprotokoll Teamviewer_Logfile), um nicht autorisierte Fernzugriffe zu erkennen.

Cybersecurity: Sicherheit der gespeicherten Daten. Datenverschlüsselung.

Der Sidexis 4 Service ist für den Zugriff auf die SQL-Datenbank mithilfe einer Authentisierung befugt.

Sicherheitsrelevante Operationen auf die Patienten- und Gesundheitsdaten werden durch Autorisierungs- und Authentifizierungsmechanismen geschützt und protokolliert. Siehe Kapitel Cybersecurity: Protokollierung der Nutzer- und System Aktivitäten. System-Log.

Sidexis 4 ermöglicht die Speicherung sensibler Patienten- und Gesundheitsdaten in einem separaten abgesicherten (ggfs. bei Bedarf verschlüsselten) Datenbereich SECURE MEDIASHARE (PDATASEC). Für die Datenverschlüsselung steht Ihnen die Verschlüsselungsfunktionalität Ihres Betriebssystems (z.B. Microsoft Windows Bitlocker) zur Verfügung. Beachten Sie, dass die Verschlüsselung größer Datenmenge zu einer Leistungsreduzierung Ihres Systems u.U. führen könnte. Sorgen Sie für eine sichere und redundante (außerhalb Ihres Systems) Aufbewahrung der Schlüssel z.B. Bitlocker-Schlüsseln und der Wiederherstellungscodes zum Backup und zur Wiederherstellung Ihrer Daten.

Prüfen Sie Ihr Sicherheitskonzept für die Segmentierung Ihrer lokalen Rechnernetzwerke (IT-Netzwerke), die Zuordnung von Datenbereichen MEDIA SHARE (PDATA) und SECURE MEDIA SHARE (PDATASEC) zu Ihren IT-Netzwerken und die Definition von Benutzerzugriffskontrollen für die Sidexis 4 Software einschließlich des befugten Zugriffs auf die Datenbanken.

Nähere Informationen über die Provisionierung von den Sidexis 4 Datenbanken, die Konfiguration von Datenbackups für die SQL-Datenbank und die Medien-Datenbanken MEDIA SHARE (PDATA) und SECURE MEDIA SHARE (PDATASEC) und mögliche Strategie für eine Datenreparatur finden Sie im Servicehandbuch Sidexis 4.

Eine regelmäßige Sicherung (Backup) der Patienten- und Gesundheitsdaten wird empfohlen. Siehe Kapitel Cybersecurity: Datensicherheit. Verfügbarkeit der Daten und Datensicherung (Backup)

Cybersecurity: Sicherheit der Daten auf dem Kommunikationsweg. Datenverschlüsselung. Autorisierung der Nachbarsysteme.

Sidexis 4 erfordert eine sichere Datenübertragung (HTPPS-Datenverschlüsselung) für den internen Austausch von Patienten- und Gesundheitsdaten zwischen den Komponenten von Sidexis 4 z.B. Intra-/Extra-oral Komponenten oder mit externen Kommunikationsknoten z.B. das Patientenverwaltungssystem (PVS) einer Klinik.

Die Kommunikation mit dem Sidexis Client und Server über eine Schnittstelle erfolgt erst nach erfolgreicher Autorisierung und Authentifizierung der Schnittstelle und der damit verbundenen Kommunikationsknoten (Nachbarsysteme).

Falls Sie einen Netzwerk-Ordner (Netzwerkshare) für die SLIDA Kommunikation angelegt haben, erfolgt die SLIDA Kommunikation über SMB (ab SMB 2.0 mit Verschlüsselung) auf Netzwerkseite, um die Integrität Ihrer Patienten- und Gesundheitsdaten zu gewährleisten.

Eine Authentifizierung der Kommunikationsknoten (Nachbarsysteme) findet neben der Autorisierung ihrer Komponenten zur Durchführung bestimmter Operationen im Sidexis 4 statt. Die Autorisierung und Authentifizierung der Nachbarsysteme erfolgt mittels eines spezifischen Applikationsschlüssels und eines Sicherheitszertifikats. Unsichere Nachbarsysteme werden in eine Sperrliste (Blackliste) durch die Sidexis 4 Konfiguration vermerkt.

Ungesicherte Kommunikationsschnittstellen zu den Nachbarsystemen können jederzeit abgeschaltet werden. Siehe *Cybersecurity: Authentisierung der Systemkomponenten und Abschaltung von unsicheren Schnittstellen*

Die Kommunikation zwischen Sidexis Client und Server erfolgt über REST-basierte Dienste unter Verwendung von HTTPS-Protokoll mit zusätzlichen Sicherheitsmaßnahmen für die Datenintegrität z.B. Datenverschlüsselung und Authentisierung der Kommunikationsknoten.

Der Zugriff auf die bereitgestellten HTTPS-Web-Schnittstellen zwischen den Application Services von Sidexis 4 und den Nachbarsystemen erfolgt grundsätzlich via SSL/TLS-sichere Verbindungen. Hierzu werden Zertifikate eingesetzt und automatisch auf den zu benutzenden Sidexis-Client-PCs registriert.

Cybersecurity: Authentifizierung der Sidexis 4 Komponenten. Sicherheitszertifikate.

Sidexis 4 verwendet Sicherheitszertifikate (X509) für folgende Zwecke:

- um die Authentifizierung der Sidexis 4 Komponenten mittels einer digitalen Signatur (Zertifikat) zu ermöglichen
- um eine verschlüsselte Datenkommunikation zwischen den Sidexis 4 Komponenten (Zertifikatsinhaber) z.B. zwischen Sidexis 4 Client und Sidexis 4 Server zu gewährleisten

Cybersecurity: Schutz gegen Schadsoftware und Manipulation, Authentifizierung und Integritätsprüfung für Sidexis 4.

Sidexis 4 verfügt über ein Tool (Integrity Checker) zur Nachprüfung der Datenintegrität der Sidexis 4 Software-Distribution (*.dll und *.exe Dateien).

Das Tool ist verfügbar in den Sprachen Deutsch (DE), Englisch (EN), Italienisch (IT), Französisch (FR) und Spanisch (ES). Das Tool verwendet die ausgewählte Sprache in Ihrem Windows-Rechner und Englisch als Standardeinstellung.

Sie finden das Tool Integrity Checker (Dateinamen: IntegrityChecker.exe) sowohl auf dem Installationsverzeichnis Ihrer Sidexis Server- und/oder Client-Installation als auch im Windows Startmenü unter dem Verzeichnis SIRONA neben der Sidexis 4 Software.

Das Tool Integrity Checker prüft mit Hilfe einer *Whiteliste* (Autorisierungsregister):

- die Datenintegrität jeder DLL oder EXE Einzeldatei mit Hilfe einer kryptografischen Hash Funktionalität (Check-Summen) und einer digitalen Signatur (Zertifikat)
- die Gültigkeit jeder einzelnen Signatur (Zertifikat)

Die Integritätsprüfung erfolgt stets auf Aufforderung des Nutzers entweder automatisch über die Kommandozeilenkonsole von Windows oder manuell über die Bedienungsoberfläche von Sidexis 4 (siehe Abbildungen unten). Jeder Windows-Benutzer darf das Tool ausführen.

Das Tool selbst ist gegen eine potenzielle Manipulation Dritter geschützt.

Zur Integritätsprüfung ist keine Eingabe von Parametern erforderlich. Das Tool übernimmt das Installationsverzeichnis von Sidexis 4 als Datenpfad für die Integritätsprüfung.

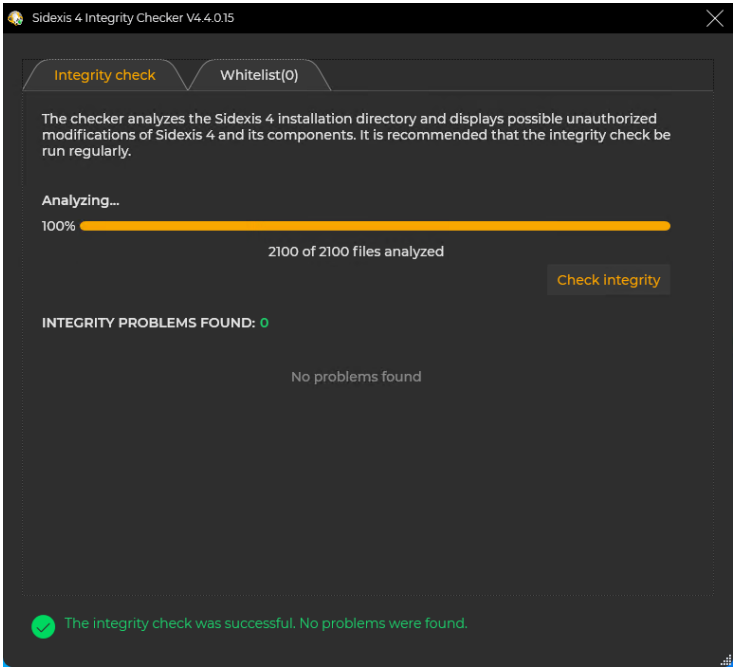
Während der Integritätsprüfung werden die Installationsdateien gescannt und Ihre Integrität untersucht. Die gefundenen Integritätsverletzungen (*Integrity Issues)* werden auf der Bedienungsoberfläche oder ggfs. auf der Windows-Kommandozeilenkonsole angezeigt.

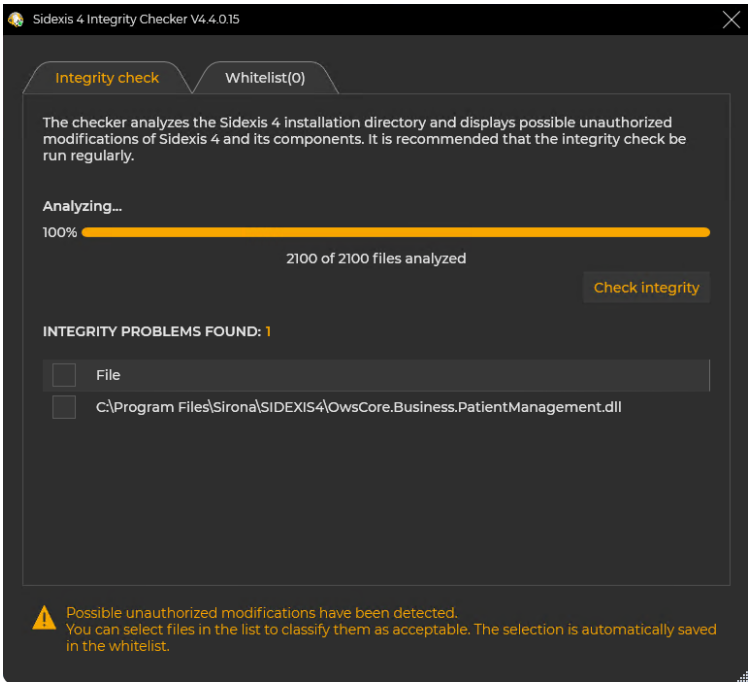
Es besteht auch die Möglichkeit, Ihre Bewertung der gefundenen Integritätsverletzungen (*Integrity Issues)* für bestimmte unbekannte Module oder Tools als plausible (falsche positive) Integritätsverletzungen (*Accepted Issues*) in eine Whiteliste (Autorisierungsregister) dauerhaft einzutragen. Dafür sind Administrator-Rechte erforderlich.

Beim Vorhandensein von nicht plausiblen Integritätsverletzungen, empfehlen wir Ihnen eine umgehende Reparaturinstallation (Repair Installation) von Sidexis 4, um eine potenzielle Kompromittierung der Sidexis 4 Software zu verhindern.

Die Integritätsprüfung von Sidexis 4 Software sollte in regelmäßigen Abständen für einen effizienten Schutz gegen Schadsoftware erfolgen. Führen Sie die Prüfung aus dem Installationsverzeichnis heraus durch, am besten, bevor Sidexis 4 das erste Mal am Tag gestartet wird.

Weitere Information über das Tool „Integrity Checker“ sind in dem Installationshandbuch zu finden.





Cybersecurity: Authentisierung der Systemkomponenten und Abschaltung von unsicheren Schnittstellen

Sidexis 4 verfügt über Sicherheitsmaßnahmen, die eine zertifikatbasierte Authentisierung der Nachbarsysteme / Systemkomponenten von Sidexis 4 und die Abschaltung unsicherer Schnittstellen ermöglichen.

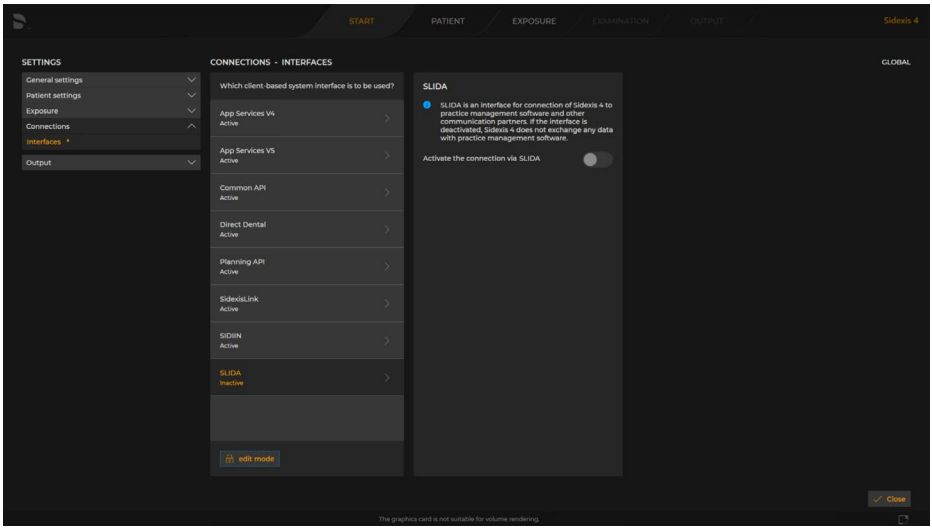
Bei abnormaler Ausführung von Sidexis 4, beim Anwenderverdacht einer Schadsoftware oder zur Entfernung von nicht autorisierten Kommunikationsknoten (Nachbarsysteme) aus der Sidexis Systemkonfiguration, lassen sich nach Absprache mit der DENTSPLYSIRONA Service-Hotline folgende Kommunikationsschnittstellen (Knoten/Nachbarsysteme) zu Sidexis 4 individuell ein- und abschalten:

- SLIDA

- Direct Dental
- Sidexislink
- SIDIIN
- AppService V4
- AppService V5
- Common API
- Planning API

Im Konfigurationsmenü „Settings – Connectivity – Interfaces“ können Sie die Ein- und Abschaltung der Kommunikationsschnittstellen zu Sidexis 4 verwalten.

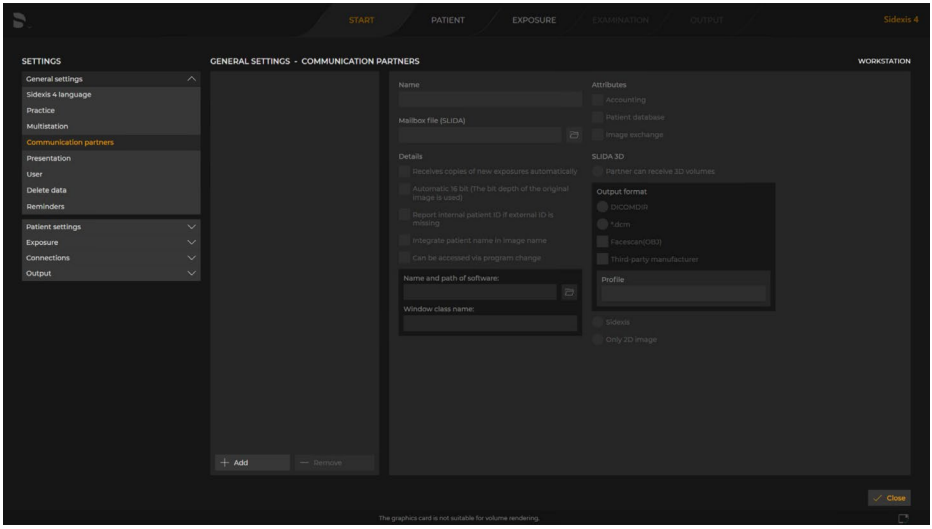
Zum Abschluss der Sidexis 4 Installation können durch den Service-Techniker weitere Sicherheitsmaßnahmen wie z.B. die Abschaltung unsicherer Schnittstellen zur zusätzlichen Absicherung (Hardening) der Sidexis 4 Software durchgeführt werden.



Für die Abschaltung einer potenziell unsicheren Schnittstelle ist die Eingabe des Sidexis 4 Administrator Passwortes erforderlich.

Hinweis: Die Abschaltung einer Schnittstelle wird die Verfügbarkeit der über die Schnittstelle verfügbare Funktionalität folglich beeinträchtigen bzw. unverfügbar machen.

Im Konfigurationsmenü „General Settings – Communication Partners“ können Sie die Einstellungen der Kommunikationsschnittstellen (Communication Partners) zu Sidexis 4 definieren.



Cybersecurity: Datensicherheit. Verfügbarkeit der Daten und Datensicherung (Backup)

Stellen Sie stets die Verfügbarkeit und Belastbarkeit Ihrer IT-Systeme, IT-Rechnernetze und Daten MEDIA SHARE (PDATA) und SECURE MEDIA SHARE (PDATASEC) sicher:

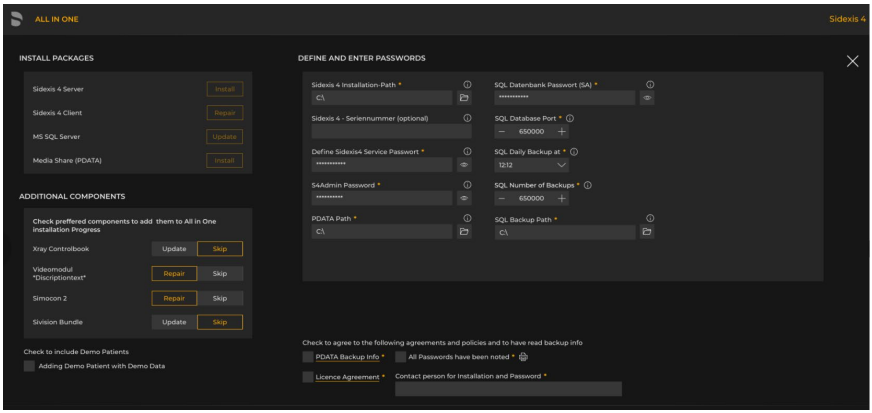
- Erhöhen Sie die Verfügbarkeit durch die Nutzung von redundanten Systemen, z. B. RAID Systeme
- Erstellen Sie Datenbackups für MEDIA SHARE (PDATA) und SECURE MEDIA SHARE (PDATASEC) in regelmäßigen Zeitabständen. Führen Sie

beide Daten-Backups zu dem gleichen Zeitpunkt durch, um eine temporale Datenkonsistenz von PDATA und PDATASEC zu garantieren.
  - Das Backup der MS SQL-Datenbank wird bei der Installation des Sidexis 4 Servers automatisch eingestellt und erfolgt infolgedessen automatisch.
  - Eine Datei-Sicherung (File-Backup) von lokal gespeicherten Patienten- und Gesundheitsdaten ist möglich und erfolgt auf dem gesicherten Datenbereich SECURE MEDIA SHARE (PDATASEC) und dem ungesicherten Datenbereich MEDIA SHARE (PDATA). Dieses Backup muss durch den Betreiber eingestellt werden und durch den verantwortlichen CERT (Beauftragter für Medizinproduktesicherheit, Medical-IT Risk Manager u.a.) regelmäßig überprüft werden.
  - Konfigurieren Sie die Dateisicherung mit einer entsprechenden Sicherungssoftware und beachten Sie dabei, dass alle Dateien und Unterordner gesichert werden müssen.
  - Achten Sie dabei auf die zeitliche Abfolge, so dass Sie die Sicherung der SQL-Datenbank in Ihre Dateisicherung mitsichern können.
  - Prüfen Sie regelmäßig das Wiederherstellen eines vorhandenen Backups und die Plausibilität der Backup-Daten auf einem Test-Server nach.
    - ➔ Tipp: Überwachen Sie die Datei ERRORLOG zu finden unter "%ProgramFiles%/Microsoft SQL Server\MSSQL14.Sidexis_SQL\Log" für (nicht) erfolgreiche Backup Aktionen.
- Prüfen Sie Ihr Sicherheitskonzept für die Segmentierung Ihrer lokalen Rechnernetzwerke (IT-Netzwerke), die Zuordnung von Datenbereichen MEDIA SHARE (PDATA) und SECURE MEDIA SHARE (PDATASEC) zu Ihren IT-Netzwerken und die Definition von Benutzerzugriffskontrollen für die Sidexis 4 Software einschließlich des befugten Zugriffs auf die Datenbanken.

Nähere Informationen über die Provisionierung von den Sidexis 4 Datenbanken, die Konfiguration von Datenbackups für die SQL-Datenbank und die Datenbanken MEDIA SHARE (PDATA) und SECURE MEDIA SHARE (PDATASEC) und mögliche Strategien für eine Datenreparatur finden Sie im Servicehandbuch Sidexis 4.

- Erstellen Sie eines Notfallkonzeptes in der Form z.B. eines Notfallplans. Berücksichtigen Sie für das Notfallkonzept folgende Aspekte:

- Die wichtigsten Risiken für Ihre Geschäftsprozesse und Ressourcen und Ihre Risikostrategien dafür
- Berücksichtigen Sie die Risiken aus der Daten- und Informationssicherheit im Notfallplan wie z.B. Datenverlust durch beschädigte Festplatte oder keine Verfügbarkeit durch Ausfall Ihrer IT-Netzwerken.
- Entwicklung einer Kontinuitätsstrategie, die einen Wiederanlauf und eine Wiederherstellung Ihrer Geschäftsprozesse in der geforderten Zeit ermöglichen.
- Planen Sie ein Schulungskonzept für das Thema Notfallmanagement und Datensicherheit für Ihr Personal



Quelle: Installationshandbuch Sidexis 4

Cybersecurity: Wartung von Sidexis 4 (Maintenance)

Fernwartung

Ein unsicherer Fernwartungszugang kann unbefugtes Eindringen in Ihre IT-Systeme und Ihre Daten verursachen. Dadurch können Manipulationen Ihrer Software und Datenverluste entstehen. Definieren und verwenden Sie Fernwartungszugänge mit viel Vorsicht, wie folgt:

- Legen Sie am besten in einer Richtlinie fest, wie Fernwartung zu erfolgen hat u.a.: welche Aktivitäten zu überwachen sind, welche Zieldaten zu bewahren sind und wie die Kommunikationsverbindungen geschützt werden sollen.
- Überprüfen Sie wo und wann Fernwartungen unbedingt notwendig sind und erlauben Sie Zugriff an den entsprechenden Arbeitsstationen nur für den benötigten Zeitraum und für die zu wartende Systemkomponente.
- Vereinbaren Sie einen rechtlich bindenden Vertrag über Fernwartungen mit Ihrem Dienstleister und kontaktieren Sie Ihren Verantwortlichen für IT-Sicherheit bzw. Ihren Beauftragten für Medizinproduktesicherheit oder Ihren Medical-IT Risikomanager.
  Tipp: Überprüfen Sie die Authentizität des Servicedienstleisters. Fragen Sie nach Informationen, die nur Ihr Dienstleister kennen kann, z. B. Ihre Kundennummer.
- Überwachen Sie die Fernwartungszugänge und dokumentieren Sie jeden Vorgang.
  Tipp: Nehmen Sie die Fernwartung als Video auf (dies benötigt unter Umständen die Zustimmung Ihres Dienstleisters).
- Prüfen Sie nach der Fernwartung die Audit-Logdatei für jeden Fernwartungszugang.
  Siehe Kapitel *Cybersecurity: Benutzerzugriffskontrollen. Audit-Log Protokollierung*

Bereitstellung und Installation von Software- und Sicherheits-Updates

Dentsply Sirona | SIRONA Dental Systems GmbH als Hersteller wird im Rahmen ihrer Entwicklungs- und Marktüberwachungs- und Meldungsprozesse die Wartung von der Sidexis 4 Software über ihren gesamten Produktlebenszyklus gewährleisten.

Die Wartungsmaßnahmen werden dem Kunden in der Form von Software-Updates zur Verfügung gestellt. Die Wartungsmaßnahmen umfassen jegliche Art von adaptiven (*adaptive*), perfektiven (*perfective*), korrektive (*corrective*) oder präventive (*preventive*) Software-Änderungen sowohl für die Produktfunktionalität (Update) als für die Produktsicherheit (Sicherheitsupdate) auch.

Dentsply Sirona | SIRONA Dental Systems GmbH als Hersteller informiert ihre Kunden durch ihr eigenes Vertriebsnetz und ihre Händler weltweit über verfügbare Software-Updates einschließlich Installationsanweisungen und stellt diese zum Download in einem abgesicherten und zugangsbeschränkten Bereich (Händlerbereich) auf dem offiziellen Online-Portal bereit.

Potenzielle IT-Security (Cybersecurity) Vorkommnisse (*Incidents*) werden regelmäßig im Rahmen der Tätigkeiten für die Marktüberwachung und das Sicherheitsmanagement von der Sidexis 4 Software in Zusammenarbeit mit relevanten Wirtschaftsakteuren (Betreiber, Händler, Importeure, Anwender) überwacht, bewertet und bei Bedarf als Sicherheitsupdate bereitgestellt.

Zur Überwachung der Cybersecurity Vorkommnisse (Security Incidents/ Vulnerabilities) sind zusammen mit dem Hersteller auch sämtliche Wirtschaftsakteure (Betreiber, Händler, Importeure) im Rahmen ihrer Geschäftsprozesse für Post-Market Surveillance und Security Incident Management verpflichtet.

Für die Installation von Software-Updates in Sidexis 4 brauchen Sie Administrator-Zugriffsrechte. Weitere Informationen über die Installation von der Sidexis 4 Software sind im Installationshandbuch zu finden.

Cybersecurity: Sicherheitsmanagement. Allgemeines.

Prüfen Sie Ihr Sicherheitskonzept und Ihre Sicherheitsmanagementstrategie nach mit Ihren Verantwortlichen für Risikomanagement und IT-Sicherheit (Cybersecurity) regelmäßig, um die Eignung und die Wirksamkeit der Sicherheitsmaßnahmen zu bestätigen.

Nachfolgend finden Sie einige nützliche Tipps (keine vollständige Liste):

IT-Infrastruktur

- Schutz gegen Schadsoftware: Virenschutzprogramm
  Nutzen Sie eine professionelle Antivirensoftware auf allen Computern (Arbeitsstationen) innerhalb Ihres lokalen Rechnernetzwerkes (IT-Netzwerk) und scannen Sie alle Informationen sämtlicher Datenquellen (USB-Stick, CD-ROM/DVD, Webseiten, Emails

einschließlich Anhänge u.a.).
Sorgen Sie für eine regelmäßige Aktualisierung und eine geeignete Konfiguration des Virenschutzprogrammes für das Betriebsfeld von Sidexis 4 hinsichtlich der Datenintegrität, des Datenschutzes und der Leistungsauslegung Ihrer IT-Systeme. Nur Nutzer mit Administrator-Zugriffsrechten sollen eine sicherheitsrelevante Änderung der Programmeinstellungen vornehmen.

- Betriebssysteme (O.S.):
  Nutzen Sie nur erprobte Versionen von Betriebssystemen auf allen Computern (Arbeitsstationen) innerhalb Ihres lokalen Rechnernetzwerkes (IT-Netzwerk), die für einen sicheren und interoperablen Betrieb mit Sidexis 4 freigegeben wurden (Siehe Sidexis 4 Systemanforderungen).
  Wir empfehlen Ihnen ältere Versionen der Betriebssysteme trotz der Interoperabilität mit Sidexis 4 zu vermeiden, um Risiken wegen potenziell fehlenden Sicherheitsfunktionen und -Einstellungen zu vermeiden.
  Desgleichen sind Zusatzsicherungsmaßnahmen (*Hardening*) für die Betriebssysteme zu empfehlen wie folgt (keine vollständige Liste):
    - Unnötige Dienste, Anwendungen und Netzwerkprotokolle zu deaktivieren oder ggfs. zu entfernen.
    - eine sorgfältige Konfiguration der Benutzerauthentifizierung Ihres Betriebssystems mithilfe einer Sicherheitsrichtlinie
    - eine restriktive Ressourcensteuerung (Zugriff auf Ressourcen wie Software und Daten)

  Sorgen Sie dafür, dass Sie relevante Sicherheitsupdates des Originalherstellers vom Betriebssystem für die für Sidexis 4 freigegebenen Versionen (Betriebssystem) auf allen Computern installieren.

- Firewall:
  Nutzen Sie eine Firewall, um Ihr lokales Rechnernetzwerk (IT-Netzwerk) zu sichern. Erlauben Sie einen Zugriff auf Ihre lokalen Rechnernetze und Ihre Rechner nur im Ausnahmefall (*secure by default*) und regeln Sie in einer Firewall-Richtlinie, wie eingehende und ausgehende Daten in Ihre Netzwerke vorgesehen sind.

Limitieren Sie Internetzugang auf ein Minimum.

Berücksichtigen Sie die sicherheitstechnischen Zusammenhänge der Firewall-Konfiguration und der Fernwartung. Die Gruppe der berechtigten Benutzer für die Fernwartung soll durch die Zuweisung entsprechender Benutzerrechte und in der Benutzerzugriffskontrolle und in der Firewall Sicherheitsrichtlinien festgelegt werden.

Prüfen Sie die Firewall-Regeln für Verbindungen von und zu Druckern, Kopierern und Multifunktionsgeräten aus dem Internet nach, um eine Kompromittierung Ihrer lokalen Rechnernetze (IT-Netzwerke) zu verhindern.

Aktualisieren Sie alle Netzwerkkomponenten regelmäßig (z. B. Router).

Software von Drittanbietern (3rd.Party)

Installieren und nutzen Sie Software von Drittanbietern nur, wenn diese zur Arbeit in der zahnmedizinischen Praxis benötigt wird.

Nutzen Sie nur aktuelle Versionen einschließlich sämtlicher verfügbaren Sicherheitspatches.

Prüfen Sie regelmäßig nach, ob Schwachstellen für die Software von Drittanbietern identifiziert wurden. Siehe nachfolgendes Kapitel.

Tipp: Wählen Sie eine Sicherheitssoftware, die Sie aktiv über bereitstehende Sicherheitsupdates von Drittanbietersoftware informiert.

Management von Schwachstellen (Vulnerabilities)

Im Rahmen Ihres Sicherheitsmanagements empfehlen wir Ihnen, eine spezifische Richtlinie für das IT Security Incident und Vulnerability Management zu gestalten.

Für eine effiziente Beschreibung und Kategorisierung der Schwachstellen und Software Defekten steht Ihnen z.B. das Regelwerk ANSI/AAMI SW91:2018 *Classification Of Defects In Health Software* zur Verfügung.

Prüfen Sie regelmäßig die öffentlich verfügbaren Informationen über Schwachstellen nach. Wir empfehlen Ihnen folgende führende Informationsquellen:

- NIST Vulnerability Database (NVD): https://nvd.nist.gov
- The MITRE Corporation Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org/cve/search_cve_list.html Migration auf https://www.cve.org/ aktuell laufend
- BSI (Deutschland), CERT-Bund Meldungen: https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Warnmeldungen/warnmeldungen_node.html

Literatur und Hilfsmittel

Wir empfehlen Ihnen weltweit verfügbare nützliche Informationen und Empfehlungen über IT-Sicherheit (Cybersecurity) für Ihre Sicherheitsanalysen und Entscheidungen heranzuziehen, wie z.B.:

- Das Computer Security Resource Center (CSRC) des U.S. National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications/sp
- Das IT-Grundschutz-Kompendium und Standards des Bundesamtes für Sicherheit in der Informationssicherheit (BSI):BSI - IT-Grundschutz-Kompendium (bund.de)
- Agentur der Europäischen Union für Cybersicherheit (ENISA): ENISA (europa.eu)

5 System Informationen

Dieses Kapitel gibt einen Überblick über das Sidexis 4 System und beschreibt alle relevanten Informationen für IT-Administratoren, um Sidexis 4 sicher in einem lokalen Rechnernetzwerk einzurichten.

Kurzer Überblick zu Sidexis 4:

Verwendungszweck, Indikation und Kontraindikation

Diese Informationen können dem **Sidexis 4 Anwenderhandbuch** (REF 6774579) entnommen werden.

Freigabe

Das Produkt trägt die CE-Marke gemäß der Europäischen Verordnung für Medizinprodukte 2017/745 (MDR).

Vorgesehenes Betriebsumfeld (*intended operational environment of use*)

Das Sidexis 4 System besteht aus zwei System-Komponenten: ein Server und ein Client als sogenannte Client-Server-Lösung, die als Einzelplatz- oder als Mehrplatzsystem betrieben werden kann.

Der reibungslose und qualitative Betrieb eines lokalen Rechnernetzes (Local Area Network/LAN) erfordert uneingeschränkte Konformität mit den im Gebäude vorherrschenden elektrischen Installation laut der international anerkannten Standards ISO/IEC 11801, der Europäischen Standards EN 50173 und EN 50174, der deutschen Standards VDE 0800-173 und 0800-174 oder des Nordamerikanischen Standards EIA/TIA 568 A/B, die vom genannten Basisstandard abgeleitet sind. Gleichzeitig müssen auch die Netzwerkverbindungen zu Röntgen-Komponenten des Herstellers überwacht werden.

Die Konfiguration eines lokalen Rechnernetzes (IT-Netzwerkes) ist von großer Bedeutung für ein sicheres Betriebsumfeld, auch als *intended operational environment of use* von der Begleitdokumentation für Cybersecurity MDCG 2019-16 zur Verordnung (EU) 2017/745 (MDR) bezeichnet, und für die Daten- und Informationssicherheit (Cybersecurity), wie im Kapitel *Überblick Systemumgebung: IT-Netzwerke, Netzwerk-Zonen und sichere Kommunikationsverbindungen (Conduits)* kurz erläutert.

Neben den Anforderungen an die Cybersecurity für das Betriebsumfeld, sind weitere Anforderungen an die Systeminteroperabilität für das Betriebsumfeld zu berücksichtigen. Siehe Definition von *Interoperabilität* im Kapitel *Definitionen laut (EU) Verordnung 2017/745 (MDR).*

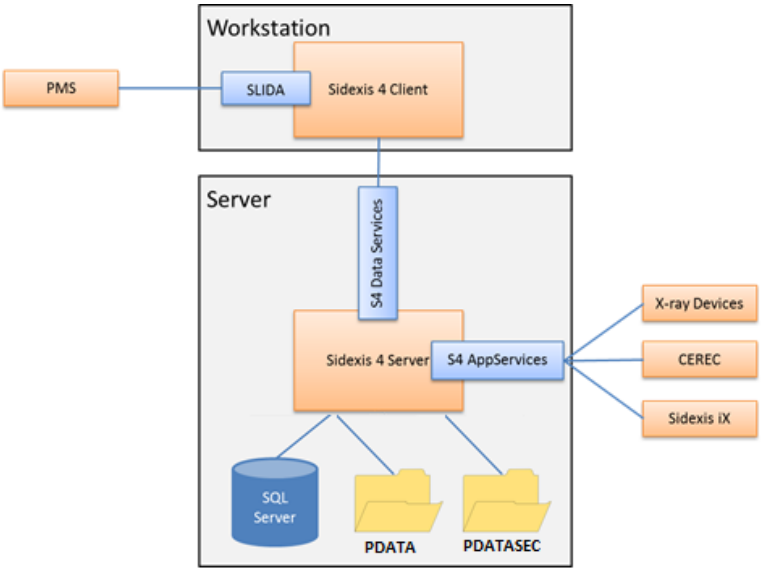
Die Umsetzung eines globalen gewünschten Grads an Interoperabilität (*Interoperabilitätsebene*) für sämtliche Medizinprodukte in einem Betriebsumfeld bzw. in einem IT-Netzwerk obliegt der Verantwortung des Betreibers, der Gesundheitseinrichtung und ggfs. des Medical-IT Risikomanagers.

Systemvoraussetzungen

Bitte überprüfen Sie stets die aktuellen Systemvoraussetzungen unter www.dentsplysirona.com/sidexis-4-system-requirements

Technischer Überblick

Die folgende Darstellung zeigt sowohl die Komponenten des Sidexis 4 Systems: Software-Komponenten Client- und Server, Datenbank-Komponenten MEDIA SHARE (PDATA) und SQL-Server als auch die Netzwerk-Schnittstellen auf, die zur Anbindung von Praxisverwaltungssystemen (PVS), Röntgengeräten, CEREC Software und Sidexis iX bereitgestellt werden.



Sidexis 4 System Komponenten	
Software	
Sidexis 4 Client *Dateiname:* sidexis4.exe *Prozessname:* Sidexis4	Die ausführbare Datei namens **Sidexis4.exe** stellt die Client-Komponente von der Sidexis 4 Software dar, die im Zielordner Ihrer Softwareinstallation auf der/den jeweiligen Arbeitsstation/-en (PC) zu finden ist. Es wird empfohlen, keine Administratorzugriffsrechte für den normalen Gebrauch von der Sidexis 4 Software auf Ihrem Rechner zu nutzen. Standard-Nutzerrechte sind ausreichend.
Sidexis 4 Server	Die ausführbare Datei namens **SidexisRestService.exe** stellt die

Dateiname: SidexisRestService.exe *Prozessname:* Sidexis4service	Server-Komponente (Service) von der Sidexis 4 Software dar, die im Zielordner Ihrer Softwareinstallation auf der jeweiligen Arbeitsstation (PC) zu finden ist. Der Sidexis 4 Server (Service) wird während der Installation auf Ihrem lokalen Rechner mit automatischem Systemstart konfiguriert. Es wird empfohlen, keine Administratorzugriffsrechte für den normalen Gebrauch vom Sidexis 4 Software auf Ihrem Rechner zu nutzen. Standard-Nutzerrechte sind ausreichend. *Empfehlung:* Erlauben Sie keine Fernzugriffe auf den Sidexis 4 Server (Service).
Datenbanken	
Sidexis 4 SQL-Server (Instanz) Microsoft SQL-Server *Prozessname:* ▪ SIDEXIS_SQL ▪ PDATA_SQLEXPRESS Schnittstellen: ▪ Microsoft SQL Server 2017 Express ▪ Open Database Connectivity (ODBC)	Der Microsoft SQL-Server wird benutzt, um Patienten- und Gerätedaten auszulesen, zu schreiben und danach zu suchen. Ausgeschlossen sind hier Mediendateien (z. B. Bilder, DVTs). Während der Nutzung von Sidexis 4 werden alle Aufrufe der SQL-Server Instanz vom Sidexis 4 Server durch die Software-Komponente NHibernate durchgeführt. Einige ältere Komponenten, wie z. B. das Konstanzprüfungsprogramm SiConst, nutzen die SQL-Server Instanz über die ODBC Verbindung. Die Microsoft SQL-Server Instanz “ SIDEXIS_SQL” wird während der Installation des Sidexis 4 Servers mit

	den folgenden Einstellungen installiert und konfiguriert: • Authentifizierung: SQL Server und Windows Authentifizierungsmodus • Login Audit: fehlgeschlagene Anmeldungen Tipp: Siehe Kapitel *Cybersecurity: Protokollierung der Nutzer- und System Aktivitäten. System-Log*. • Netzwerk-Konfiguration: • Shared Memory: Enabled • Named Pipes: Disabled • TCP/IP: Enabled <u>Benutzer-Konten - User Access Management</u> • **SQL SA Passwort:** Passwort für den Service-Administrator der SIDEXIS SQL-Datenbank Instanz • **Sidexis 4 Service (Sidexis4Service) Passwort:** Passwort für den Windows-Benutzer "Sidexis4Service" des Sidexis 4 Services (Servers) • **Sidexis 4 Admin (S4Admin) Passwort:** Passwort für Admin-Benutzer im Sidexis 4 für den Zugriff auf geschützte Einstellungen und sensible Funktionen (wie z.B. Medien verschieben oder Patient löschen) von Sidexis 4 <u>Sicherung der Daten</u> Nutzen Sie die von Sidexis 4 bereitgestellten Möglichkeiten zum

	regelmäßigen Datenbackup der SQL-Datenbank. Hinweis: Der Sidexis 4 SQL-Server verwendet kommerzielle Software Drittanbietern (Off-the-shelf-Software/OTS) und zwar die Komponente SQL Server 2017 Express.
Sidexis 4 MEDIA SHARE (PDATA) *Dateien-Ordner oder Netzwerkshare:* PDATA	Die dateibasierte Datenbank MEDIA SHARE (PDATA) wird vom Sidexis 4 Server zum Speichern von allgemeinen Daten (keine sensiblen Daten!), Datenkonfigurationen und Installationsressourcen genutzt. *Empfehlungen:* ▪ Gewähren Sie Nutzern Zugriffsrechte auf die Ordnerfreigabe (Netzwerkshare) PDATA nur, falls dies essentiell für Aufgaben im Zusammenhang mit dem Sidexis 4 System notwendig ist. ▪ Achten Sie insbesondere darauf, keine Zugriffsrechte auf die Ordnerfreigabe (Netzwerkshare) MEDIA SHARE (PDATA) für Nutzer über Fernzugriff bzw. Fernwartung einzuräumen. ▪ Sorgen Sie für regelmäßige Datenbackups.

Sidexis 4 SECURE MEDIA SHARE (PDATASEC) *Dateien-Ordner oder Netzwerkshare:* PDATASEC	Die dateibasierte Datenbank SECURE MEDIA SHARE (PDATASEC) ist für die gesicherte Speicherung von sensiblen Daten wie die Gesundheits- und Patientendaten, Medien-Daten (z.B. Aufnahmen, DVTs, DICOMs), Metadaten und Sitzungen durch Sidexis 4 vorgesehen. Dafür ist eine Einrichtung dieses sicheren Datenbereiches auf Ihrem Rechner mithilfe von der Verschlüsselungssoftware Ihres Betriebssystems (z.B.Microsoft Windows Bitlocker) erforderlich. Achten Sie bitte auf eine sichere und redundante Speicherung (möglichst außerhalb Ihres Rechners auf einem separaten Speichermedium) der Verschlüsselungsschlüsseln (z. B. Bitlocker) und der Wiederherstellungscodes. Eine Datenwiederherstellung trotz vorhandenen Backups ohne die Bitlocker Schlüsseln und die Wiederherstellungscodes ist nicht möglich. *Empfehlungen:* Falls Sie die dateibasierte Datenbank SECURE MEDIA SHARE (PDATASEC) als Netzwerk-Ordner (Netzwerkshare) auf Ihrem IT-Netzwerk freigegeben haben, achten Sie auf Folgendes: ▪ Gewähren Sie nur dem Sidexis 4 Service (Server) Zugriffsrechte auf den Netzwerk-Ordner (Netzwerkshare) SECURE MEDIA SHARE (PDATASEC) ▪ Achten Sie insbesondere darauf, keine Zugriffsrechte auf den Netzwerk-Ordner

	(Netzwerkshare) SECURE MEDIA SHARE (PDATASEC) für Nutzer über Fernzugriff bzw. Fernwartung einzuräumen. ▪ Sorgen Sie für regelmäßige Datenbackups.
Schnittstellen	
SLIDA	SLIDA ist eine Schnittstelle basierend auf einer Datei-basierten Kommunikation (I/O Operationen, SLIDA Eingangs-/Ausgangsdatei) zwischen der Sidexis 4 Software und der Software von Drittanbietern, wie z. B. Praxisverwaltungssystemen. Für jede Richtung der Kommunikation wird eine SLIDA Eingangs- und Ausgangsdatei normalerweise in einem lokalen Ordner auf dem Rechner abgelegt, auf den beide Kommunikationspartner zugreifen können. Falls Sie einen Netzwerk-Ordner (Netzwerkshare) für die SLIDA Kommunikation angelegt haben, erfolgt die SLIDA Kommunikation über SMB mit Verschlüsselung auf Netzwerkseite. . *Empfehlung:* Nutzen Sie für jede SLIDA Eingangs- und Ausgangsdatei einen Ordner, der nur für bestimmte Nutzer sichtbar und zugänglich ist, um die entsprechenden Sidexis 4-Tätigkeiten ausführen zu können
Sidexis 4 Dataservices	Dieser Service-Endpoint wird vom Sidexis 4 Server bereitgestellt, um

	dem Sidexis 4 Client Datenzugriff zu ermöglichen. Transport Layer Security (TLS) wird mit dem höchstmöglichen Protokoll geschützt, das zwischen Client und Server ermittelt wird. Je nach Kombination von Server und Client-Betriebssystem führt dies zu SSL 3.0, TLS 1.2 oder TLS 1.3 Die Data Endpoints greifen auf den Port 42928 und auf 42930 mit einem selbst-erstellten Zertifikat.
Sidexis 4 AppServices V4 AppServices V5 AppServices V6	Dieser Service-Endpoint wird durch den Sidexis 4 Server bereitgestellt, um Röntgengeräten und Applikationen, wie z. B. Sidexis iX und CEREC Software Zugang zu High Level Daten (Workflows, Patienten, Medien, Konfiguration) zu gewähren. *Hinweis über AppServices Versionen:* Für Sidexis V4.4 ist eine sichere Datenübertragung (Transport Layer Security/TLS) und eine Komponentenauthentifizierung vorhanden. Die beste mögliche SSL/TLS Version ausgehandelt (SSL 3.0, TLS 1.0 – TLS 1.3) wird ausgehandelt. Die Service-Endpoints dieser Versionen greifen auf die Ports 42929 (AppServices V4 und V5) und 42931 (AppServices V6) mit einem selbsterstellten Zertifikat zu.
Direct Dental	Client-Schnittstelle zur Anbindung von „Sidexis XG Geräte/Softwareplugins

SidexisLink	Schnittstelle zur Anbindung von Dentsply Sirona Komponenten z.B. Dentrix an das Praxisverwaltungssystem (PVS)
SIDIIN	Low-Level Schnittstelle zu Dentsply Sirona-Röntgengeräten. Erzeugte Daten werden in der PVS weiterverarbeitet.
SiTwain	TWAIN 2.2 -Schnittstelle zu Dentsply Sirona-Geräten
Abschaltung unsicherer Schnittstellen	Siehe Kapitel Cybersecurity: Sicherheit der Daten auf dem Kommunikationsweg. Datenverschlüsselung. Autorisierung der Nachbarsysteme.
Betriebsumfeld: Nachbarsysteme	
Sperre (Blackliste) unsicherer Schnittstellen	Sidexis 4 verfügt über eine vorkonfigurierte Funktionalität zur Sperre (Blacklisting) von unsicheren Schnittstellen. Der Sperrmechanismus wird systematisch mit den Produkt-Updates aktualisiert. Siehe Kapitel Cybersecurity: Sicherheit der Daten auf dem Kommunikationsweg. Datenverschlüsselung . Autorisierung der Nachbarsysteme.

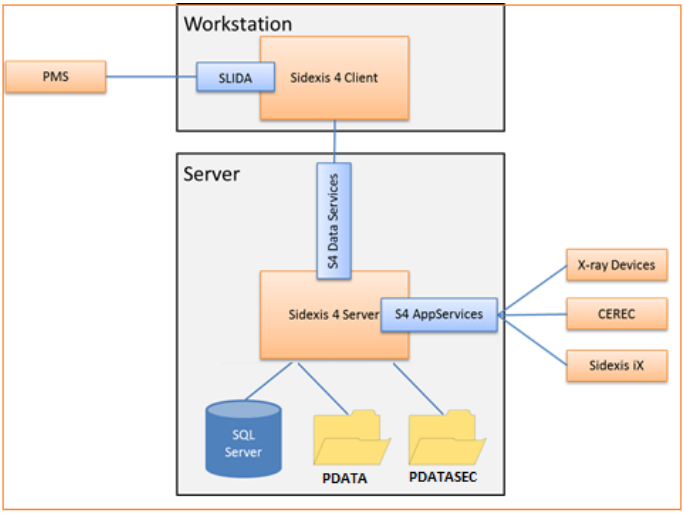
Überblick Systemumgebung: IT-Netzwerke, Netzwerk-Zonen und sichere Kommunikationsverbindungen (Conduits)

Die folgenden nicht-vollständigen Darstellungen zeigen einige Beispiele möglicher Konfigurationen Ihrer IT-Netzwerke und des Sidexis 4 Systems. Die IT-Netzwerke werden unten mit einem orangen Rahmen dargestellt.

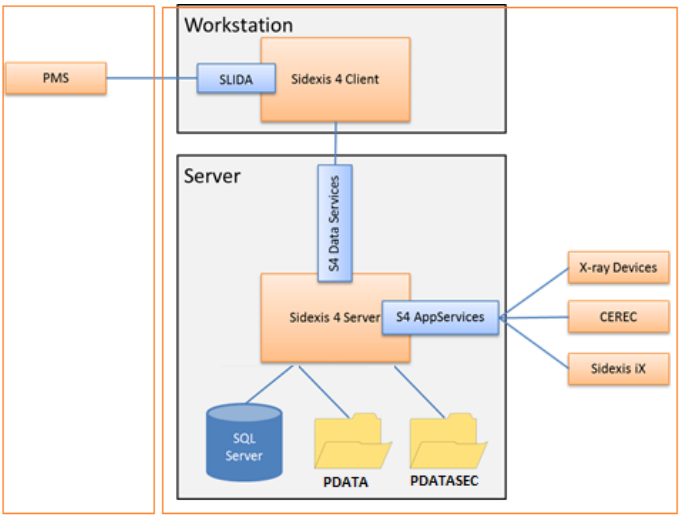
Achten Sie bitte darauf, dass Ihre IT-Netzwerke von Ihrem IT-Administrator in Abstimmung mit Ihrem Beauftragten für Medizinproduktsicherheit und ggf. Ihrem Medical-IT Risikomanager sicher konfiguriert werden. Sie finden nützliche Informationen über eine sichere Konfiguration von IT-Netzwerken im Industrie-Standard *DIN EN IEC 62443 IT-Sicherheit für industrielle Automatisierungssysteme (Security for industrial automation and control systems)*. Der Standard IEC 80001-1:2021 hilft Ihnen zusätzlich mit der Anwendung von Best-Practices zum Risikomanagement für die IT-Netzwerke in Ihrer Organisation.

Die Konfiguration unterschiedlicher Sicherheitszonen in einem IT-Netzwerk (Netzwerksegmentierung) genauso wie die Nutzung von einer Netzwerkzone DMZ für Außenschnittstellen, Sicherheitsroutern und – Firewalls mit sicheren Kommunikationsverbindungen (Conduits) und einer Anti-Virus Software wird für eine sichere Nutzung vom Sidexis System und den Schutz Ihrer Patientendaten empfohlen. Dies kann nur erfolgen, wenn die Integrität Ihres lokalen Rechnernetzes mittels Zugriffskontrollen für die verschiedenen Netzwerk-Segmente gewährleistet ist.

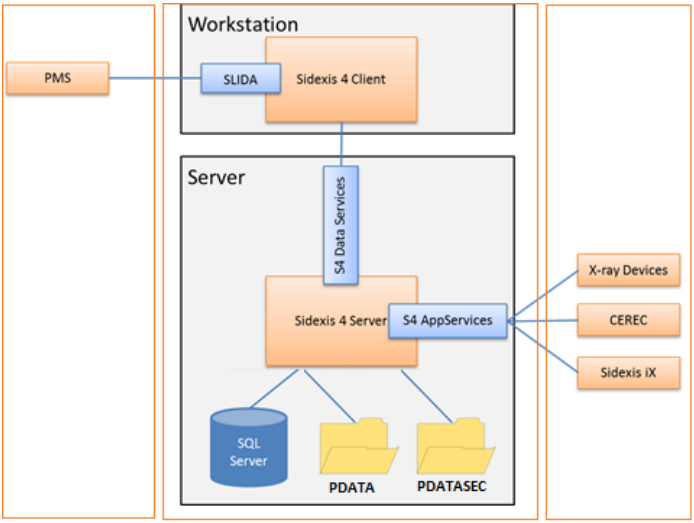
Beispiel 1: nur ein IT-Netzwerk für alle Systeme



Beispiel 2: Zwei IT-Netzwerke. Eins für Ihr PMS und eins für sämtliche Komponenten des Sidexis-4 Systems und der Röntgenkomponenten



Beispiel 3: Mehrere IT-Netzwerke zur Trennung von den PMS, Sidexis-4 Client und Server, und den Röntgenkomponenten.



Eine sichere Segmentierung und Konfiguration Ihrer IT-Netzwerke ist von großer Bedeutung für den Schutz der Sidexis Software und Ihrer Gesundheits- und Patientendaten auch während der Datenübertragung (Transmission Confidentiality, Transmission Integrity) zwischen den IT-Netzwerken.

6 Rechtlicher Hinweis / Haftungs-ausschluss

Rechtlicher Hinweis / Haftungsausschluss

Bitte beachten Sie, dass dieses Whitepaper zum Thema „Datenschutz und Produktsicherheit“ kein Ersatz für rechtliche Beratung ist, wie die Anforderungen an Datenschutz und/oder Produktesicherheit einschließlich Cybersecurity der Europäischen Verordnungen zu erfüllen sind.

Der Autor übernimmt keinerlei Gewähr für die Aktualität, Richtigkeit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.