Leistungsverzeichnis für das qualified Trust Repository (qTR) von DMI mit DPaaS qT

1. Übersicht

Dieses Dokument beschreibt das qualified Trust Repository (qTR) von DMI als Grundlage der Clinical Document and Data Services von DMI. In diesem Repository werden Informationen aus der Behandlungsdokumentation hochstrukturiert und interoperabel aufbereitet und vorgehalten und den verschiedenen Diensten aus der Familie der Clinical Document and Data Services zur Verfügung gestellt.

Das qTR speichert die medizinischen Behandlungsinformationen in einer konsolidierten Patientenakte. Diese enthält die elektronischen und digitalisierten, interoperabel nach den Vorgaben von FHIR und IHE klassifizierten Dokumente aus dem Behandlungsfall sowie strukturierte Daten. Durch den in der qTR-Leistung enthaltenen Bewahrungsdienst nach eIDAS „DPaaS qT“ werden die betreffenden Inhalte integritätsgesichert. Dieser Dienst ist untrennbarer Bestandteil des qualified Trust Repositories von DMI.

Der Zugang zu den mit dieser Leistung abgelegten medizinischen Informationen erfolgt über Applikationen oder Schnittstellen aus der Familie der Clinical Document and Data Services, z.B. können über das von DMI betriebene intuitive Frontend „Cloudviewer“ diese Informationen den Anwendenden präsentiert werden. Das „Dashboard“ bietet auf der Basis der gespeicherten Metadaten Statistiken rund um den Grad der Digitalisierung an. Ob und in welcher Weise und in welchem Umfang die vorgehaltenen Datenarten dann weiter genutzt werden, ist nicht Bestandteil dieses Leistungsverzeichnisses.

Das qualified Trust Repository wird in den Secure Datacentern von DMI betrieben. Damit stellt es an den IT-Betrieb des Kunden minimale Anforderungen.

Die hier in diesem Dokument beschriebene Leistung umfasst das Vorhalten sowie die Integritätssicherung der Daten.

Zielsetzung und Nutzen

In einem dynamischen Umfeld, in dem sich Prozesse und Vorgaben schnell ändern, gibt es einen Aspekt, der konstant bleibt: behandlungsrelevante Informationen sind aufbewahrungspflichtig!

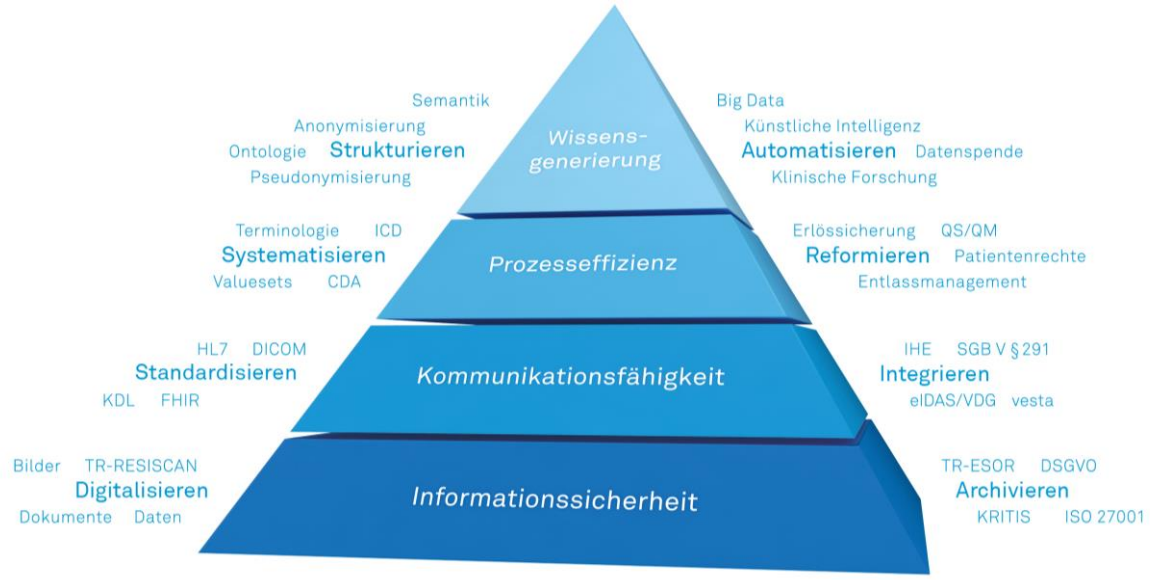

Abbildung 1: Bedürfnispyramide des Archivar 4.0

Dies bedeutet, dass trotz aller Digitalisierungsbestrebungen und der damit einhergehenden hohen Dynamik, die Fragen der Informationssicherheit mitgedacht werden müssen. Dazu gehören neben den Überlegungen zur Archivierungs- und Digitalisierungsstrategie auch Fragen der Verfügbarkeit behandlungsrelevanter Informationen und deren Beweiswerterhaltung über die Dauer der Aufbewahrungsfrist.

Digitale Daten allein genügen nicht, um digitale Prozesse effizient umzusetzen. Möglich wird dies erst durch die Nutzung etablierter und offener Standards sowohl im Bereich der Kommunikationstechnologien als auch im Bereich der interoperablen Gestaltung der Daten für diese Prozesse.

Durch die Nutzung des qTR von DMI wird eine Grundlage geschaffen, auf der zukunftssichere Prozesse aufgebaut werden können, die auf integren, interoperablen Daten basieren.

2. Methodik und Voraussetzung

Die integritätsgesicherte Datenhaltung beinhaltet folgende Informationen:

- Patienten- und Fallstammdaten aus HL7-ADT-Nachrichten
- Dokumente im gängigen PDF-, TIFF-, PNG oder JPEG-Format, die über HL7-MDM Nachrichten an DMI ausgeleitet werden
- Metadaten der digitalisierten Behandlungsdokumentation mit automatisierter Dokumententypklassifizierung, inkl. KDL-Klassierung
- Metadaten der zugehörigen elektronischen Dokumente, inkl. KDL-Klassierung

Nach Eintreffen der Nachrichten werden die gelieferten Dokumente und Metadaten zunächst unverändert der Langzeitarchivierung DPaaS Classic zugeführt.

In der anschließenden Aufbereitung der Nachrichteninhalte werden die Einzelinformationen unter Berücksichtigung öffentlicher Codesysteme und ValueSets, wie sie in FHIR-Profilen verwendet werden, strukturiert abgelegt. Maßgeblich sind hier vor allem die Spezifikationen zum ISiK Basismodul in der aktuellen Ausbaustufe sowie der Medizininformatikinitiative und der KBV.

Für Dokumente erfolgt zusätzlich die Anreicherung mit Metadaten aus dem Musterordner des Kunden, um das Dokument sowohl in der klinischen Registerstruktur als auch in der Struktur weiterer Ontologien wie der KDL vorzuhalten.

Voraussetzungen

Administrativ	• Onboarding des Kunden mit seinen relevanten Namespaces und Prozessen
Notwendige Services	• digitaler Musterordner mit aktuellen krankenhausindividuellen, papierbasierten und elektronischen Dokumenten, die für die Behandlungsdokumentation verwendet werden (patientenanonymisiert) mit Qualifizierung nach Klinischer Dokumentenklassen-Liste (KDL) • empfohlen: Digitalisierung und Dokumententypindexierung papierbasierter Behandlungsdokumentation mit Dokumentenbindung
Kundenseitige Voraussetzungen	• Elektronische Dokumente liegen gebunden vor.

3. Leistungsbeschreibung Aufnahme und Vorhalten der Daten im qTR

Im Rahmen der Projektinitiierung werden zunächst die Datenströme in der Kundenumgebung betrachtet, um die Quellsysteme für die Ausleitung der Daten aus der Kundenumgebung zu den Clinical Document & Data Services (CDDS) im DMI Secure Data Center festzulegen. Dabei ist unerheblich, welches DMS in der Kundenumgebung als Quellsystem eingesetzt wird.

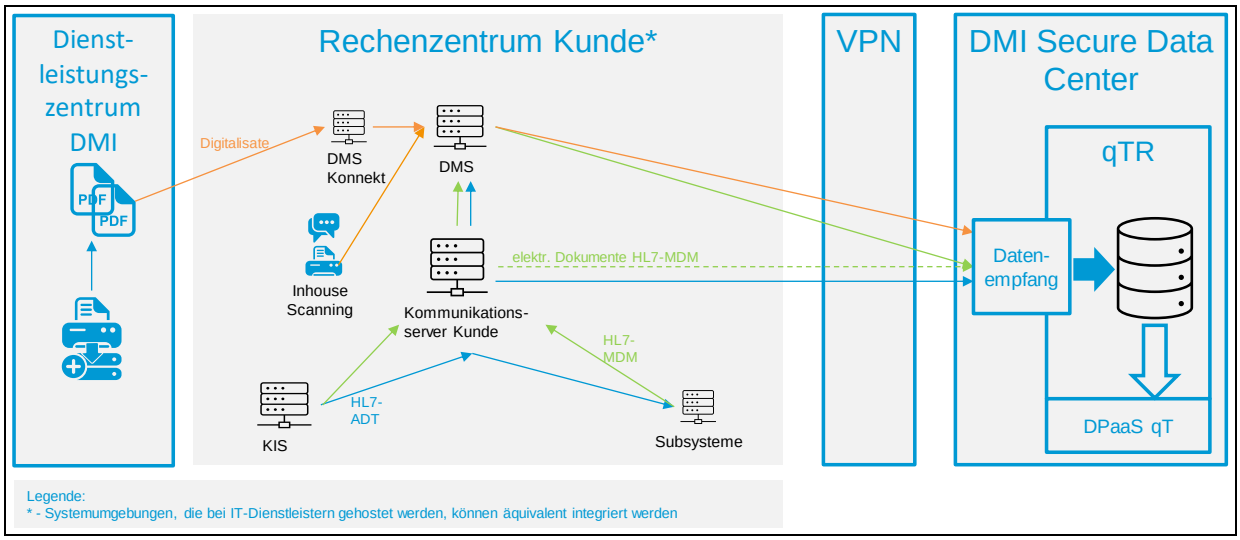

Abbildung 2: Datenstrom Kundenumgebung -> CDDS mit beliebigem DMS

- HL7-ADT:
  - Ausleitung direkt aus dem Kommunikationsserver des Kunden
  - In begründeten Ausnahmefällen kann eine Ausleitung aus AVP Komms eingerichtet werden. In diesem Fall wird der Einsatz von mindestens AVP Infinity als DMS in der Kundenumgebung vorausgesetzt.
- HL7-MDM:
  - Ausleitung aller in das eingesetzte DMS eintreffenden Dokumente unabhängig von der Quelle des Dokuments

Maßgeblich für die Inhalte der HL7-ADT und HL7-MDM-Schnittstellen ist die Schnittstellenspezifikation von DMI. Projektspezifische Abweichungen sollen in der Regel vermieden werden, sind aber in begründeten Einzelfällen möglich.

Die in den von DMI empfangenen Nachrichten enthaltenen Dokumente und Metadaten werden noch vor deren Aufbereitung und Weiterleitung an das qualified Trust Repository der Langzeitarchivierung zugeführt (siehe Leistungsverzeichnis „Revisionssichere Langzeitarchivierung DPaaS und Durchführung der Revision“). Im Rahmen der Nachrichtenaufbereitung werden im Anschluss die Informationen in eine FHIR-ähnliche Struktur überführt und angereichert. Die Ablage der Daten erfolgt in hochstrukturierter Form im qualified Trust Repository von DMI.

Berücksichtigung von Bestandsdokumenten

Grundsätzlich ist die Ausleitung bereits vorhandener Dokumentbestände in der Umgebung des Kunden für die Nutzung der CDDS möglich. Im Projekt ist zu prüfen, inwiefern die Metadaten der Dokumente den Anforderungen der Schnittstellenspezifikationen genügen. Eine Übernahme großer Dokumentbestände ist nicht Bestandteil dieses LV und gesondert anhand der vorliegenden Rahmenbedingungen abzustimmen und zu beauftragen.

4. Leistungsbeschreibung Integritätssicherung - Digital Preservation as a Service – qualified Trust (DPaaS qT)

Die Daten und entsprechenden Integritätsnachweise werden im Rahmen des DMI Bewahrdienstes gesichert. Die Integritätssicherung ist Bestandteil der qTR-Leistung. Die Details dieser Leistung ergeben sich aus diesem Kapitel. DMI bietet für die übernommen Daten und Dokumente einen Vertrauensdienst zur Bewahrung des Beweiswertes von qualifizierten elektronischen Signaturen und Siegeln bzw. Dokumentationen, mit denen diesen versehen sind.

Kernmerkmal: Zertifiziertes Produkt

Für diesen Dienst hat DMI Teile seiner Leistungen als elektronischen Bewahrungsdienst gem. eIDAS Verordnung Art. 34 qualifizieren lassen. Dies erfolgte durch die **Zertifizierung nach ETSI TS 119 511**. Das zu diesem Zweck eingesetzte Produkt ist nach **BSI TR-03125 (TR-ESOR)** zertifiziert.

Hinweis

In diesem Leistungsverzeichnis werden die Funktionen von DPaaS qT genannt und kurz umschrieben. Zentraler Baustein von DPaaS qT ist das zu diesem Zweck eingesetzte, zertifizierte TR-ESOR Produkt. Es gelten daher zusätzlich zu diesem Leistungsverzeichnis alle zum Zertifizierungszeitpunkt (Feststellung der Konformität) des TR-ESOR Produktes gültigen dbzgl. Dokumente.

Funktionen

Grundlage für die Nutzung des Bewahrungsdienstes und seiner im Folgenden genannten Funktionen ist die zuvor beschriebene Ablage der Dokumentation und Daten im qualified Trust Repository von DMI. Der Bewahrungsdienst selbst hält die Integritätsmerkmale für diese Dokumentation und Daten.

Ablage digitaler Dokumentation (ArchiveSubmission)

Die Funktion Ablage (Submission) ermöglicht die Ablage eines Archivcontainers (L)XAIP zu den zugehörigen Daten. Dabei handelt es sich um die Behandlungs- und Pflegedokumentation im qTR.

Ändern archivierter digitaler Dokumentation / Versionierung (ArchiveUpdate)

Die Funktion zur Aktualisierung von archivierter digitaler Dokumentation, z.B. Patienten / Fall Behandlungs- und Pflegedokumentation ermöglicht das Hinzufügen oder die Veränderung von Primärdaten und ggf. Metadaten, sowie die Ablage des diesbezüglich versionierten Archivcontainers (L)XAIP im qTR.

Abfrage archivierter digitaler Dokumentation (ArchiveRetrieval)

Die Funktionen ArchiveRetrieval ermöglicht den Abruf einzelner archivierter Datenelemente digitaler Dokumentationen oder auch die gesamte Dokumentation z.B. in Bezug auf Patienten und / oder deren Behandlungsfälle.

Löschen (ArchiveDeletion)

Mit der Funktion Archive Deletion können eine oder mehrere archivierte digitale Dokumentationen z.B. in Bezug auf Patienten und / oder deren Behandlungsfälle gelöscht werden. Es wird vor Löschung geprüft, ob die festgelegte Mindestaufbewahrungsfrist abgelaufen ist. Sofern es sich um ein Löschen vor dem Ablauf der Aufbewahrungsfrist handelt, muss vor Löschung eine Begründung für die Löschung protokolliert werden.

Rückgabe technischer Beweisdaten (ArchiveEvidence)

Die Funktion Rückgabe technischer Beweisdaten (ArchiveEvidence) ermöglicht den Abruf eines Evidence Records bzw. Beweisdatensatzes zum Nachweis der Authentizität und Integrität von einem oder mehreren im qTR abgelegten (L)XAIP, sowie der zugehörigen Daten, z.B. Patienten / Fall Behandlungs- und Pflegedokumentationen.

Abruf von Bewahrungsprofilen / Preservation Profiles

Die Funktion Abruf von Bewahrungsprofilen gibt die im TR-ESOR ArchiSafe Modul gespeicherten Bewahrungsprofile (Preservation Profiles) zurück.

Abruf von Log-Daten

Die Funktion Abruf von Log Daten gibt die im TR-ESOR ArchiSafe-Modul gespeicherten Log Daten zurück.

Schaubild

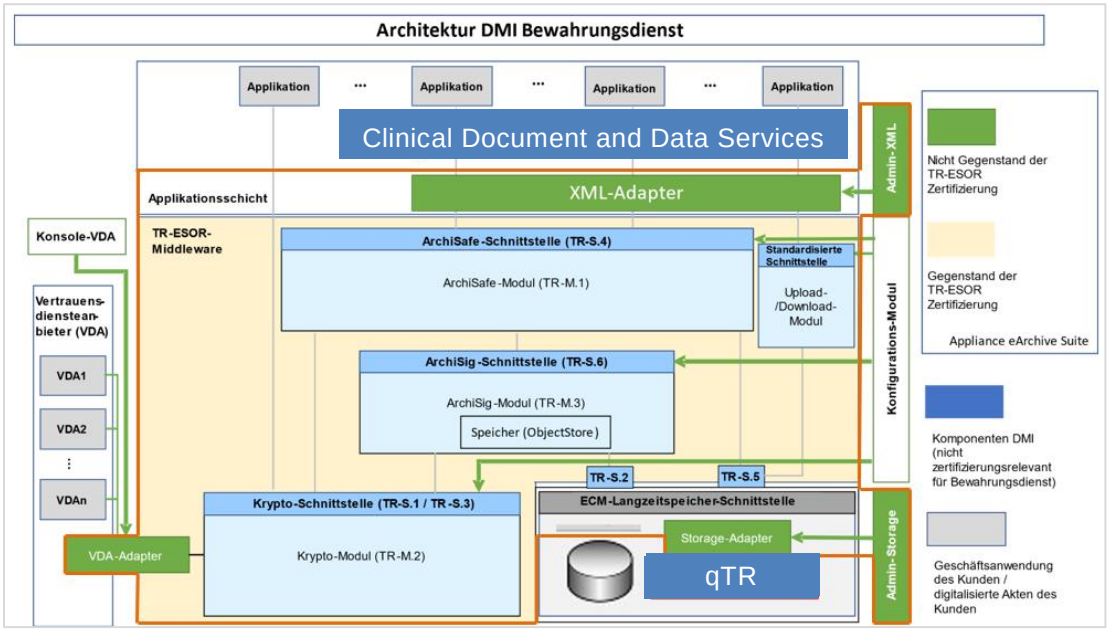

Abbildung 3: Architektur des DMI-Bewahrungsdienstes

Sichtbarkeit für den Kunden

In der ersten Ausbaustufe von DPaaS qT handelt es sich ausschließlich um einen Backend-Service. Aus dem Grund ist dieser für Kunden nicht sichtbar. Die oben aufgeführten Funktionen sind daher auch nicht direkt für Kunden erreichbar.

Aufbewahrung von Ereignisprotokollen

Die Aufbewahrungsdauer der Ereignisprotokolle des Bewahrungsdienstes entspricht mindestens der Bewahrungsdauer des integritätsgesicherten Objektes.

Abruf von Integritätsnachweisen durch Kunden

In der ersten Ausbaustufe von DPaaS qT können Integritätsnachweise zu im qTR abgelegten Daten ausschließlich kostenpflichtig seitens des Kunden über den DMI-Anforderungsservice angefordert werden.

Abruf von Ereignisprotokollen

In der ersten Ausbaustufe von DPaaS qT können Ereignisprotokolle zu im qTR abgelegten und durch den Bewahrungsdienst integritätsgesicherten Daten ausschließlich kostenpflichtig seitens des Kunden über den DMI-Anforderungsservice angefordert werden.

5. Gewährleistung der Datenschutzanforderungen nach DSGVO

Verarbeitete Daten

Das System verarbeitet personenbezogene Daten aus zwei Gruppen von Personen:

1. Daten von Patienten: Verarbeitet werden die für die Ausleitung bestimmten und über die HL7- Schnittstellen gelieferten Patientendaten. Diese Daten werden nach Art, Inhalt und Umfang durch den Kunden im Rahmen des Schnittstellenkonzepts festgelegt. Alle medizinischen Informationen haben mindestens einen Patientenbezug; in der Regel auch einen Behandlungsbezug.

2. Daten von Nutzern: Mitarbeitende des Kunden haben auf den Datenbestand weder Zugang noch Zugriff. Es werden keine Daten von dieser Personengruppe verarbeitet. Aktivitäten der DMI-Systemadministration werden über die entsprechenden Tools protokolliert. Die zugrundeliegenden Prozesse sind im Datenschutzkonzept von DMI dokumentiert.

Umsetzung der Datenschutzgrundsätze

Beim Betrieb werden die Datenschutzgrundsätze in folgender Weise sichergestellt:

Zweckbindung & Rechtmäßigkeit	• Patientendaten: Zweck der Verarbeitung personenbezogener Daten ist das Vorhalten der Patientendaten für Zwecke des Auftraggebers (integritätsgesicherte Datenhaltung). Dies schließt die Vorhaltung für weitere Data Services sowie die Integritätssicherung der gespeicherten Daten (siehe Abschnitt, Kapitel 4) ein. • Nutzerdaten: Festgelegter Zweck ist der Nachweis der korrekten Verarbeitung der Daten und Aufklärung eventueller Vorkommnisse sowie zu Zwecken der Fehlerkennung und -behebung. • Die Verarbeitungsmöglichkeiten unterliegen den getroffenen Regelungen in der mit der Leistungsvereinbarung abgeschlossenen Vereinbarung zur Auftragsverarbeitung.
Speicherbegrenzung	• Patientendaten: Die Speicherung der Daten erfolgt im Standard 30 Jahre beginnend mit dem Entlassungsdatum zum Behandlungsfall, zu dem die Daten jeweils gehören. Die Löschung erfolgt nach einem spezifischen Löschkonzept. • Es können kundenindividuell vom Standard abweichende Löschfristen vereinbart werden. Die Löschung einzelner Dokumente/Daten, für die keine Verwahrung mehr erfolgen soll, ist möglich; dies erfolgt durch Erstellen eines Auftrags (Tickets) an DMI und dem manuellen Löschen der Verweise auf diese Dokumente/Daten.
Vertraulichkeit und Verfügbarkeit	• Die Verfügbarkeit und Vertraulichkeit der gespeicherten Daten wird durch Anwendung der spezifischen DMI IT-Sicherheitskonzepte für die CDDS gewährleistet. • Alle Maßnahmen sind im Betriebskonzept und den technisch organisatorischen Schutzmaßnahmen festgelegt.

Integrität

- Die geschützt gespeicherten Patientendaten werden mit dem in diesem Leistungsverzeichnis beschriebenen Dienst integritätsgesichert. Die Integritätssicherung ist Ziel dieser Leistung.

Umsetzung der Betroffenenrechte des Patienten

Die Wahrung der Betroffenenrechte für Patienten obliegt dem Kunden. Über eine Mitteilung an DMI können Kunden im Namen ihres Patienten ein Betroffenenrecht geltend machen.

Recht auf Auskunft über gespeicherte Daten (Art. 15 DSGVO)

- Bei entsprechender Anfrage des Patienten kann eine autorisierte Person des Kunden auf Antrag gegenüber DMI einen Export der Akte mit allen gespeicherten Inhalten zum betreffenden Patienten erhalten. Autorisierte Stellen und Wege sollten in der Auftragsverarbeitungsvereinbarung festgelegt werden.

Recht auf Berichtigung (Art. 16 DSGVO)

- Korrekturen von Stammdaten des Patienten können in den führenden Systemen der Kundenumgebung (Klinikumgebung) vorgenommen werden. Über die oben beschriebene Stammdatenschnittstelle HL7-ADT werden Änderungen an diesen Daten an DMI gemeldet und an die angeschlossenen Services weitergeleitet.

- Korrekturen an Dokumenten erfolgen ebenfalls in der Kundenumgebung (Klinikumgebung) und werden analog über die HL7-MDM Schnittstelle an DMI übertragen.

Recht auf Löschen (Art. 17 DSGVO)

- Wünschen Patienten das Löschen ihrer Daten, ist die erste Ansprechstelle der jeweilige Kunde. Die Ausführung erfolgt mit Einzelauftrag des Kunden an DMI.
  Zur Umsetzung des Löschrechtes erfolgt keine Löschung einzelner Datenfelder oder einzelner Dokumente, weil dies die primäre Behandlungsdokumentation und den Sachstand zum Dokumentationszeitpunkt verfälschen würde und damit auch dem Sinn der hier beschriebenen Leistung zuwiderlaufen würde. Das Löschrecht kann nur für eine nicht mehr aufbewahrungspflichtige Primärdokumentation insgesamt gelten. Um die zu einer primären Behandlungsdokumentation gehörenden Daten von nicht zugehörigen Daten abzugrenzen, werden Daten und Dokumente jeweils in einem „Vorgang“ zusammengefasst; ein Vorgang entspricht dabei einem Behandlungsfall bzw. einer Fall-ID. Alle Daten und Dokumente eines Falls bzw. einer Fall-ID bilden einen Vorgang. Auf Anforderung bzw. Antrag des Kunden kann jeder Vorgang unabhängig von der hinterlegten Löschfrist im qTR durch DMI manuell gelöscht werden. Die Daten des Vorgangs im qTR werden auf Antrag einer autorisierten Person durch DMI manuell gelöscht. Autorisierte Stellen und Wege sollten in der Auftragsverarbeitungsvereinbarung festgelegt werden.

- Bei Ausübung der Löschfunktion wird eine E-Mail an eine fest hinterlegte Mailadresse des Kunden gesendet, um die Löschung zu bestätigen und dort zu überwachen. Das Löschen eines Vorgangs bewirkt, dass kein Dienst mehr auf diese Daten zugreifen kann.

Recht auf Einschränkung der Verarbeitung / Widerspruch zur Verarbeitung (Art. 19/21 DSGVO)

- Es obliegt dem Kunden eine Inanspruchnahme dieses Rechts gegenüber dem Patienten zu bearbeiten. Widersprüche des Patienten müssen kundenseitig in den Kundensystemen durchgesetzt werden. Dies kann über Änderungen der Daten erfolgen. Dabei wird ein entsprechendes Kennzeichen gesetzt, welches die Beschränkung von Zugriffen sowie Verarbeitung für konkrete Services auslöst.
- Ergänzend können außerdem auf Antrag des Kunden einzelne Datenfelder oder Dokumente vollständig ausgeblendet werden, indem für diese Einzeldaten Löschmarkierungen gesetzt werden. Das Setzen der Löschmarkierung bewirkt, dass auf diese Daten nicht mehr zugegriffen werden kann, auch wenn der tatsächliche Löschvorgang systemisch bedingt erst später vollständig umgesetzt ist.

6. Sonstige Hinweise

Die Prozesse zur Archivierung von Dokumentationen sind im Rahmen des zertifizierten Informationssicherheits-, Datenschutz- und Qualitätsmanagementsystem, kurz IDQMS, dokumentiert. Das System erfüllt die Anforderungen der ISO 9001, ISO/IEC 27001 und bezüglich der Digitalisierungsdienstleistung die Anforderungen der BSI TR-03138 (RESISCAN).

Die TÜV Rheinland Group sowie weitere unabhängige Auditoren prüfen regelmäßig im Rahmen von Überwachungs- und Rezertifizierungsaudits die Erfüllung der Normen sowie die Einhaltung der Datenschutzgrundverordnung (EU-DSGVO).

Die Archivierung erfolgt ausschließlich durch geschultes und ausgebildetes Fachpersonal.
Alle Beschäftigten von DMI sind hinsichtlich des Datenschutzes und Informationssicherheit geschult sowie gemäß §203 Strafgesetzbuch zur Einhaltung der Schweigepflicht verpflichtet.

Entsprechende Service-Level-Agreements (SLA) werden dem Kunden zur Verfügung gestellt.

7. Glossar

Begriff	Beschreibung
DPaaS qT	**DPaaS q**ualified **T**rust dient als Integritätsnachweis / Beweiswerterhalt von Datenobjekten über deren Laufzeit, während der die Datenobjekte im qTR abgelegt sind.
DPaaS Classic	**D**igital **P**reservation **a**s a **S**ervice **Classic** steht für die revisionssichere Langzeitarchivierung auf Offline-Speichern (LTO Soft-WORM Band) von DMI und wird in den DMI eigenen **S**ecure-**D**ata-**C**entern betrieben. DPaaS richtet sich an alle DMI Kunden, sowohl aus den Bereichen Healthcare, als auch Non-Healthcare. DPaaS wird seit dem Jahr 2012 produktiv von einem Großteil der DMI Kunden genutzt. Mit Einführung von DPaaS qT wurde DPaaS in DPaaS Classic umbenannt.
CDDS	Die **C**linical **D**ocument and **D**ata **S**ervices bilden die logische Klammer um Workflows, Technik und Daten / Dokumente, welche die Grundlage bilden, DMI Kunden Mehrwertdienste anzubieten.
qTR	Das **q**ualified **T**rust **R**epository umfasst alle patientenbezogenen Einzelinformationen. Dazu gehören strukturierte Daten, Dokumente, Bilddaten und zugehörige Metadaten. Das qTR ist zentraler Bestandteil der CDDS.
Cloudviewer	Cloudviewer ist ein Teil der CDDS und ermöglicht den sicheren, autorisierten, browserbasierten Zugriff auf die konsolidierte Digitale Patienten-Dokumentation im qTR.
XAIP	**X**ML formatted **A**rchival **I**nformation **P**ackage Ein Archivdatenobjekt, d. h. ein für die langfristige Ablage in einem elektronischen Bewahrungs- bzw. Archivsystem bestimmtes elektronisches Dokument im Sinne der TR-ESOR, ist ein selbst-beschreibendes und wohlgeformtes XML-Dokument, das gegen ein gültiges und autorisiertes XML-Schema geprüft werden kann.
LXAIP	**L**ogisches **XAIP** (LXAIP) Ein LXAIP unterscheidet sich von einem XAIP, dadurch, dass die Inhalte, d.h. die Sequenz der Elemente xaip:dataObject aus der xaip:dataObjectsSection, xaip:metaDataObject aus der xaip:metaDataSection oder xaip:credential aus der xaip:credentialsSection herausgenommen werden, in separate Datenobjekte (z.B. Dateien) abgelegt werden und dafür in das XAIP eine Sequenz von Referenzen auf die entsprechenden dataObject(s), metaDataObject(s) oder credential(s) eingefügt werden, so dass im XAIP eine entsprechende Verlinkung auf die ausgelagerten Datenobjekte entsteht.
ArchiSafe-Modul	Das ArchiSafe-Modul veranlasst die Prüfung elektronischer Signaturen, Siegel, Zeitstempel und Zertifikate durch das Krypto-Modul und trägt die Ergebnisse in die Archivdatenobjekte ein, bevor diese im qTR abgelegt werden.
Krypto-Modul	Das Krypto-Modul stellt verschiedene kryptographische Funktionen bereit, die für den Beweiswerterhalt benötigt werden. Dabei handelt es sich um Funktionen, die für das Berechnen von Hashwerten, die Validierung von elektronischen Signaturen, Siegeln, Zeitstempeln, zur Nachprüfung elektronischer Zertifikate benötigt werden. Darüber hinaus verfügt es über Mechanismen zum Einholen von qualifizierten Zeitstempeln, sowie (optional) von elektronischen Signaturen und Siegeln.
DMI Secure-**D**ata-**C**enter	DMI **S**ecure-**D**ata-**C**enter; Rechenzentren von DMI; Abkürzung **DMI SDC**
Digitale Patienten-Dokumentation	Im Rahmen des DMI-Digitalisierungsprozesses entstandene Digitalisate sowie die vom Kunden bereitgestellte digital vorliegende Dokumentation. Dazu gehören: - originär elektronisch erzeugte Dokumente - strukturierte Daten, - Images (DICOM), - Von DMI und vom Kunden selbst erzeugte Digitalisate - durch den Kunden von den Patienten übernommene digitale Dokumentation