Datenschutzkonzept DETECT v3.0 [DRAFT]

Beim vorliegenden Dokument handelt es sich um ein globales Datenschutzkonzept. Es beschreibt die Software DETECT und deren datenschutzrechtlichen Aspekte. Es ist um ein lokales, klinikspezifisches Datenschutzkonzept zu erweitern.

Vorhaben

Ein wesentlicher Grund für den Organspendermangel in Deutschland ist das Erkennungsdefizit eines drohenden potentiell irreversiblen Hirnfunktionsausfalls (IHA), bei Intensivpatienten in den Krankenhäusern (1). In einer Studienauswertung von Trabitzsch/Pleul (2) konnte gezeigt werden, dass eine automatisierte Filterung der intensivmedizinischen Fälle anhand von in der Routineversorgung erfassten Prädiktoren und eine anschließende Benachrichtigung der zuständigen Transplantationsbeauftragten, zu einer signifikanten Steigerung der durchgeführten Diagnostiken des irreversiblen Hirnfunktionsausfalls führt.

Zielsetzung des Vorhabens

Darauf aufbauend soll im Projekt DETECT der implementierte Algorithmus weiterentwickelt und in weiteren Kliniken in Deutschland etabliert werden. Ziel ist eine produktnahe Anwendung, die sich in die jeweiligen Klinikinfrastrukturen (insbesondere die Datenanbindung an Patientendatenmanagementsysteme - PDMS) integrieren lässt. In diesem Zusammenhang soll der Betrieb der Software an den Kliniken getestet und die notwendigen Schnittstellen, zu den jeweils im Einsatz befindlichen Patientendatenmanagementsystemen, etabliert und weiterentwickelt werden (2).

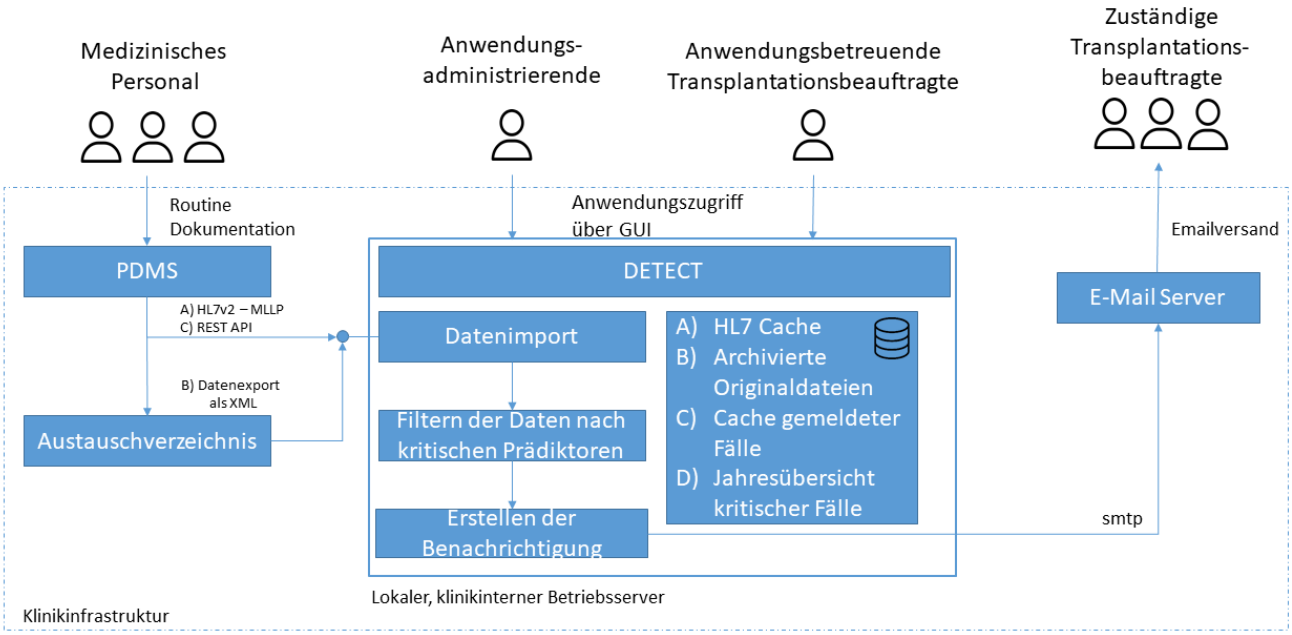
Beschreibung des Datenflusses

I) Als lokale Datenquelle dient das im Einsatz befindliche Patientendatenmanagementsystem (PDMS), in dem das medizinische Personal die Daten aus der Routineversorgung, gemäß den intensivmedizinischen Behandlungsleitlinien, erfasst. Für den Betrieb der DETECT-Software sind dabei folgende Daten zwingend erforderlich: Pupillenreaktion, Glasgow Coma Score (GCS) oder Richmond Agitation-Sedation Scale (RASS), Fallnummer (als KIS und PDMS-Nummer), sowie Position (z.B. Bettplatz- oder Zimmernummer) des Patienten. Die Fallnummer und die Position sind notwendig, damit die zuständigen Transplantationsbeauftragten den Patienten zuordnen können. Anhand der intensivmedizinischen Prädiktoren werden die Daten nach Trabitzsch/Pleul [1] gefiltert. Optional können durch DETECT weitere Parameter an den zuständigen TXB übermittelt werden, so dass dieser den Zustand des Patienten noch besser einschätzen kann. Dazu gehören: kontrollierter Beatmungsmodus, Hirndruck (ICP > 50 mmHg über 15 Minuten), kranieller Perfusionsdruck (CPP < 20 mmHg über 15 Minuten), die Serumnatriumkonzentration (Natrium <130 mmol/l bzw. >160 mmol/l, Änderung der Serumnatriumkonzentration >10 mmol/l in 24 Stunden, sowie eine stattgehabte Reanimation

II) Die Ausleitung der Daten richtet sich nach den Möglichkeiten der jeweiligen Klinik. Hierfür steht die Option der Datenausleitung als XML-Datei über ein Austauschverzeichnis oder die Datenausleitung als HL7v2-Datenstrom. In jedem Fall wird die Anwendung auf einem lokalen, klinikinternen Server betrieben (Betriebsserver), sodass die Kommunikation lediglich innerhalb des Kliniknetzwerkes stattfindet.

<table>
<tr><th>A - Datenausleitung als HL7v2-Nachricht</th><th>B - Datenausleitung als XML-Datei</th><th>C - Datenausleitung mittels REST API</th></tr>
<tr><td>II A) Am jeweiligen Standort wird eine Datenausleitung aus dem PDMS realisiert. Dazu werden die erforderlichen, medizinischen Daten und die erforderlichen personenbezogenen Daten je Fall in einer HL7v2-Nachricht zusammengefasst und der Anwendung mittels MLLP-Protokoll übermittelt.</td><td>II B) Am jeweiligen Standort wird eine Datenausleitung aus dem PDMS realisiert. Die Ausleitung sollte alle 12 Stunden durchgeführt werden. Dazu werden die gemessenen, medizinischen Rohdaten gelistet in einem strukturierten Datenformat (XML) je Intensivstation in ein klinikinternes, zugriffgeschütztes Austauschverzeichnis abgelegt, welches als Übergabepunkt zur DETECT-Anwendung fungiert. Die Anwendung überprüft viertelstündlich, ob sich eine neue Datei am Übergabepunkt befindet. Ist dies der Fall, erfolgt der Import der Datei aus dem Austauschverzeichnis durch die Anwendung.</td><td>II C) Am jeweiligen Standort wird eine Datenausleitung aus dem PDMS realisiert. Dazu werden die erforderlichen, medizinischen Daten und die erforderlichen personenbezogenen Daten je Intensivstation als strukturiertes Datenformat (JSON) an die REST-Schnittstelle von DETECT gesandt. Sobald DETECT die Daten erhält wird eine Verarbeitung der Daten ausgelöst.</td></tr>
<tr><td>III) Die erhaltenen Daten werden innerhalb der Anwendung ausgewertet. Nach dem die Nachricht in der Anwendung erhalten wurde, wird geprüft, ob kritische intensivmedizinischen Prädiktoren vorliegen. Sollte dies der Fall sein, werden die Daten in einem E-Mail-Cache gespeichert. Dieser ist eine Zusammenfassung aller kritischen Fälle pro Station. Aller 12 Stunden werden die vorgehaltenen Nachrichten versendet.</td><td colspan="2">III) Analog zu Variante A werden die erhaltenen Daten ausgewertet. Nach dem Erhalt der Daten filtert die Anwendung die Fälle nach den genannten, intensivmedizinischen Prädiktoren. Liegt ein kritischer Fall vor, werden die Fallnummern, die Positionen, sowie der Detektionszeitpunkt, d.h. wann der Fall durch die Software ausgewertet wurde, und die Empfangsemailadresse der zuständigen Transplantationsbeauftragten in einer E-Mail zusammengefasst. Anschließend wird die generierte E-Mail versendet.</td></tr>
<tr><td colspan="3">IV) Mittels einer Transportverschlüsselung via smtp-Protokoll wird eine verschlüsselte Verbindung zu dem E-Mail Server der Klinik aufgebaut. Über diese Verbindung wird die von der Anwendung erstellte E-Mail übermittelt. Der E-Mail Server versendet anschließend die E-Mail zu dem Postfach des zuständigen Transplantationsbeauftragten.</td></tr>
<tr><td colspan="3">V) Die Software speichert die Fallnummer und das Verarbeitungsdatum kritischer Fälle für 30 Tage in einem lokalen Cache innerhalb der Anwendung. Hierdurch kann DETECT innerhalb der E-Mail zwischen bereits gemeldeten und neuen Fällen unterscheiden.</td></tr>
</table>

VI) Die vorgehaltenen Nachrichten werden lediglich bis zum versenden der E-Mail vorgehalten. Anschließend werden die Daten gelöscht.	VI) Die ursprünglich importierte Originaldatei wird innerhalb der Anwendung gespeichert. Hierfür wird ein sogenanntes *docker-volume* verwendet, welches automatisch ein Verzeichnis mit beschränkten Zugriffsrechten auf dem Betriebsserver erstellt. In diesem wird die Datei abgelegt. Die Software DETECT löscht die archivierten Originaldateien standardmäßig nach 30 Tagen. Der Zeitraum ist bei der Inbetriebnahme der Anwendung nach den Vorgaben der jeweiligen Klinik anpassbar.	
VII) Es wird für jedes Jahr eine .csv-Datei als Jahresübersicht der kritischen Fälle generiert und ebenfalls in einem *docker-volume* gespeichert. In der Jahresübersicht der kritischen Fälle werden ausschließlich das Detektionsdatum, sowie die Fallnummern der gefilterten Fälle vermerkt. Die archivierte Originaldatei und die Jahresübersicht der kritischen Fälle dienen der Bewertung der Funktionalität und der Qualitätsabsicherung.		



Rollenbeschreibung der Nutzer*innengruppen

Es gibt drei Gruppen, die die Anwendung direkt nutzen. Das medizinische Personal wird in der Betrachtung ausgeschlossen, da dieses nicht in Kontakt mit der Anwendung steht.

1. *Anwendungsadministrierende*
   - sind verantwortlich für die Inbetriebnahme der Anwendung, die Betriebseinstellungen - beispielsweise die Übergabe der notwendigen Zertifikate oder die Konfiguration des Austauschverzeichnisses - sowie der Überwachung des Betriebs. Sie besitzen neben den Rechten der anwendungsbetreuenden Transplantationsbeauftragten die Möglichkeit, die Softwaremetriken wie die Anzahl an Seitenaufrufen einzusehen, neue Intensivstationen in der Anwendung einzurichten oder bestehende Stationen zu löschen, den Import der Daten manuell auszulösen, die Löschung archivierter Originaldateien sowie die Einrichtung neuer Anwendungsnutzenden. Außerdem benötigen sie Zugriffsrechte auf den internen Klinikserver, sodass sie den Betrieb der Anwendung sicherstellen können. Im Auslieferungszustand der Anwendung handelt es sich hierbei um eine Person.
2. *Anwendungsbetreuende Transplantationsbeauftragte (abTXB)*
   - sind verantwortlich für die Orchestrierung der zuständigen Transplantationsbeauftragten. Hierzu können sie mittels einer Weboberfläche festlegen, an welche Email-Adressen je Intensivstation die Anwendung eine Benachrichtigung versendet. Außerdem können sie über die Weboberfläche die Jahresübersicht der kritischen Fälle herunterladen sowie sich die Summe der versendeten Benachrichtigungen je Intensivstation und die Summe der als von der Anwendung als kritisch eingestufte Fälle je Intensivstation innerhalb eines auswählbaren Zeitraumes anzeigen lassen. Im Auslieferungszustand der Anwendung handelt es sich um eine Person, wobei neue Personen durch die Anwendungsadministrierenden hinzugefügt werden können.
3. *Zuständige Transplantationsbeauftragte (zsTXB)*
   - sind verantwortlich für die Auswertung der intensivmedizinischen Fälle je Intensivstation. Sie haben keinen Zugriff auf die Anwendung. Sie erhalten von der Anwendung eine Benachrichtigungsemail mit den gefilterten, kritischen Fällen je Intensivstation. Innerhalb der Anwendung wird die Email-Adresse der jeweiligen Person gespeichert.

Betroffener Personenkreis

Betroffene sind stationäre, intensivmedizinisch behandelte Patienten und Patientinnen mit primärer oder sekundärer Hirnschädigung in der jeweiligen Klinik. Von der Anwendung ausgeschlossen wird die Nutzung der Daten von Patienten und Patientinnen unter 18 Jahren, da hierzu noch keine Studie zu der Nutzbarkeit der Prädiktoren vorliegt.

Von Personen innerhalb der Nutzer*innengruppe *Anwendungsadministrierende* und *anwendungsbetreuende Transplantationsbeauftragte* werden keine Daten gespeichert. Von Personen der Nutzer*innengruppe *zuständige Transplantationsbeauftragte* werden die Emailadressen gespeichert.

Beteiligte Stellen

- Klinik: Die Klinik nutzt und betreibt die Software. Sie stellt die notwendige Infrastruktur, die für den Betrieb der Software notwendig ist: Betriebsserver, E-Mail Server, Patientendatenmanagementsystem. Sie ist ebenfalls für den ordnungsgemäßen und sicheren Betrieb der Infrastruktur verantwortlich. Hierbei gelten die jeweiligen, lokalen Datenschutzrichtlinien der Klinik. Außerdem benennt Sie Personen, welche als *Anwendungsadministrierende* und *anwendungsbetreuende Transplantationsbeauftragte* für den Betrieb der Anwendung in der Klinik zuständig sind. Zusätzlich ist die Klinik verantwortlich, die Ausleitung der Patientendaten aus dem Klinik-PDMS zu realisieren.
- Datenintegrationszentrum Dresden (DIZ Dresden): Feature-Entwicklung, Entwicklung von Schnittstellen zu weiteren PDM-Systemen und Unterstützung bei der Inbetriebnahme der Software.
- Deutsche Stiftung Organtransplantation (DSO): Koordinierung der Zusammenarbeit, d.h. Aggregierung von Kliniken, welche die Anwendung nutzen.

Sowohl das Datenintegrationszentrum Dresden als auch die Deutsche Stiftung Organtransplantation hat keinen Zugriff auf die Anwendung oder gespeicherte Daten innerhalb der jeweiligen Klinik.

Zugriffsberechtigte Personen

Direkten Zugriff zur Software und somit zu den archivierten Originaldateien sowie der Jahresübersicht der kritischen Fälle haben zwei Nutzergruppen: *Anwendungsadministrierende* und *anwendungsbetreuende Transplantationsbeauftragte*.

Durch das Verschicken der Benachrichtigungen erhalten die *zuständigen Transplantationsbeauftragten* Einsicht in die kritischen Fälle der jeweiligen Intensivstation. Es muss durch den *anwendungsbetreuenden Transplantationsbeauftragten* sichergestellt werden, dass die angegebenen Emailadressen tatsächlich die Adressen der zuständigen Transplantationsbeauftragten sind und die zuständigen Transplantationsbeauftragten einsichtsberechtigt in die Patientendaten der jeweiligen Intensivstation sind.

Technisch-organisatorische Sicherheitsmaßahmen

Die Software wird von der jeweiligen Klinik betrieben, sodass die Sicherheitsmaßnahmen der Klinik gelten, welche mit dem lokal zuständigen Datenschutzbeauftragten abgestimmt sind.

Absicherung der Software

Die Software wird innerhalb der jeweils lokalen Klinikinfrastruktur betrieben. Die betreibende Klinik muss den vorschriftsgemäßen Betrieb sicherstellen, d. h. das vorliegende Datenschutzkonzept muss um das lokale, kliniksspezifische Datenschutzkonzept erweitert werden. Beispielsweise folgt, dass das bereitgestellte Austauschverzeichnis der Klinik durch ein Passwort geschützt wird und lediglich die Anwendung über einen technischen Nutzer lesenden Zugriff gewährt bekommt oder der Server, auf welchem die Anwendung betrieben wird, gegen Zugriffe von außen abgesichert wird.

Die Anwendung selbst stellt einen Reverse-Proxy (TRAEFIK) bereit, welcher eine TLS-verschlüsselte Kommunikation zwischen dem Endgerät des Nutzers und den Anwendungskomponenten sicherstellt. Für Testzwecke stellt die Anwendung dafür ein selbstsigniertes Zertifikat aus. Für einen produktiven Betrieb muss der Anwendung bei der Inbetriebnahme das klinikspezifische Zertifikat zur Verschlüsselung der Kommunikation übergeben werden.

Der Zugriff auf das Austauschverzeichnis erfolgt mittels smb-Protokoll (Standard-Netzwerkfreigabe in Windows). Hierfür muss von der Klinik ein technischer Nutzer mit zugehörigem Passwort angelegt werden, welcher lesenden Zugriff auf das bereitgestellte Austauschverzeichnis besitzt. Passwort und Nutzername werden der Anwendung bei der Inbetriebnahme übergeben.

Die Kommunikation zum Email-Server erfolgt verschlüsselt mittels smtp-Protokoll. Dafür muss der Anwendung bei der Inbetriebnahme das jeweilige Zertifikat übergeben werden.

Zur Authentifizierung der Nutzer gegenüber der Software wird KEYCLOAK als zusätzlicher Service ausgeliefert und beim Start der Anwendung hochgefahren. Dabei wird mittels dem OpenID-connect Protokoll die Anwendung abgesichert. Hierbei stellt KEYCLOAK dem Nutzer bei erfolgreicher Anmeldung ein signiertes Access-Token zur Verfügung, welches die Anwendung auf Gültigkeit überprüfen kann. Alle Aufrufe der REST-API müssen autorisiert sein. Für den Authentifizierungsservice KEYCLOAK wird bei der Initialisierung der Anwendung ein Passwort generiert oder durch den Anwendungsadministrierenden festgelegt. Somit besitzt der Anwendungsadministrierende Zugriffsrechte auf den Authentifizierungsservice KEYCLOAK und kann dort neue Nutzer anlegen.

Die Anwendung ist mittels docker vollständig containerisiert und innerhalb des internen Containernetzwerkes - sowie über den Zugriff des Root-Nutzenden des Betriebsservers - oder über die nach außen definierten Schnittstellen zu erreichen. Sensible, anwendungsspezifische Daten wie Passwörter werden in sogenannten "docker-secrets" abgespeichert.

Eingabekontrolle

Die Dateneingabe findet im Kontext der Versorgung statt. Die eingegebenen Daten werden vom medizinischen Personal in der Routineversorgung erfasst und im klinikinternen PDMS dokumentiert. Innerhalb der DETECT-Anwendung findet keine Eingabe von patientenbezogenen Daten statt. Es werden keine Daten aus der Anwendung in das PDMS geschrieben.

Die Protokollierung der Aufrufe der Anwendung durch anwendungsbetreuende Transplantationsbeauftragte oder durch Anwendungsadministrierende ist mittels dem angebundenen Authentifizierungsdienst KEYCLOAK prinzipiell möglich. Hierbei würde die entsprechende Rolle, als auch das Datum des Logins erfasst werden. Im Auslieferungszustand ist diese Funktion jedoch deaktiviert und für die Nutzung der Anwendung nicht notwendig. Zugriff auf die Konfiguration des Authentifizierungsdienstes KEYCLOAK haben ausschließlich Anwendungsadministrierende.

Wiederherstellung der Verfügbarkeit bei Zwischenfall

Die gespeicherten, archivierten Originaldateien als auch die Jahresübersicht der kritischen Fälle werden auf dem klinikinternen Betriebsserver vorgehalten und durch das Backup-System des Servers gesichert. Somit können sie bei Ausfall wiederhergestellt werden. Die Verfügbarkeit wird durch das klinikspezifische Rahmenkonzept gesichert. Des Weiteren ist die Anwendung nicht kritisch für die Patientenversorgung, ein Ausfall der Anwendung ist folglich unbedenklich, selbst wenn gespeicherte Daten nicht mehr wiederhergestellt werden können. In diesem Fall ist lediglich eine Neukonfiguration des Systems erforderlich.

Zugriffskontrolle

Die Anwendung unterscheidet die oben beschriebenen Nutzerrollen. Der *Anwendungsadministrierende* besitzt vollständigen Zugriff auf die Anwendung und muss zum Zwecke der Inbetriebnahme ebenfalls Zugriffe auf den Betriebsserver besitzen. Die *anwendungsbetreuenden Transplantationsbeauftragten* hingegen besitzt lediglich Zugriff auf die Weboberfläche der Anwendung. In dieser hat er ebenfalls nur beschränkten Konfigurationszugriff, d.h. er kann lediglich Änderung an den Emailadressen durchführen. Außerdem besitzt er die Einsicht auf die archivierten Originaldateien und hat Zugriff auf den Jahresüberblick von kritischen Fällen, zu denen eine Benachrichtigung versendet wurde. Die Absicherung der Zugriffskontrolle wird durch Auswertung des signierten Access-Tokens, welches beim Login durch den Authentifizierungsdienst zur Verfügung gestellt wird, gewährleistet.

Es muss durch die *anwendungsbetreuenden Transplantationsbeauftragten* sichergestellt werden, dass die stationsspezifischen, konfigurierten Emailadressen der *zuständigen Transplantationsbeauftragten* den tatsächlich zuständigen Transplantationsbeauftragten zugeordnet und diese einsichtsberechtigt in die Patientenakten der jeweiligen Intensivstation sind.

Beschreibung der erhobenen, genutzten, verarbeiteten Daten sowie deren Erforderlichkeit

Die Anwendung nutzt Datensätze je angebundener Intensivstation. Die Arbeitsschritte i und ii müssen durch die Klinik-IT erfolgen.

Es sollen folgende Daten erfasst werden:

	Welche Daten werden erfasst?	**Wieso müssen diese Daten erfasst werden?**
erforderliche personenbezogene Daten	• Patienten-Identifikator (KIS-ID / PDMS-ID) • Position des Patienten	Die zuständigen Transplantationsbeauftragten müssen wissen, welcher Patient potentiell einen irreversiblen Hirnfunktionsausfall erleiden könnte
erforderliche medizinische Daten	• Pupillenreaktion • Glasgow Coma Score (GCS) **oder** Richmond Agitation-Sedation Scale (RASS)	Wesentliche Prädiktoren für die Filterung nach kritischen Fällen eines irreversiblen Hirnfunktionsausfalls.
optionale personenbezogene Daten	• Vor- & Nachname des Patienten	Erleichtert den zuständigen Transplantationsbeauftragten die Zuordnung der Nachricht zu einem Patienten und verkürzt die Bewertungszeit massiv.

optionale medizinische Daten	• Kontrollierter Beatmungsmodus • stattgehabte Reanimation • intrakranieller Druck (ICP > 50 mmHg über 15 Minuten) • zerebralen Perfusionsdruck (CPP < 20 mmHg über 15 Minuten) • Serumnatrium (Natrium < 130 mmol/l bzw. > 160 mmol/l) • Veränderung des Serumnatriums > 10 mmol /l innerhalb von 24 Stunden	Jeder der Faktoren kann die Einschätzung der zuständigen Transplantationsbeauftragten zu einem Patienten komplementieren, wird jedoch nur krankheitsbildspezifisch oder unzureichend erfasst. • Kontrollierter Beatmungsmodus: bei Vorliegen eines irreversiblen Hirnfunktionsausfalls ist keine Spontanatmung möglich • Reanimation: Eine stattgehabte Reanimation, kann auf die Entwicklung einer sekundären Hirnschädigung hindeuten • ICP: Ein pathologischer Anstieg des Hirndrucks über einen definierten Zeitraum ist ein Hinweis auf eine raumfordernde intrakranielle Läsion, ein Hirnödem oder eine Liquorzirkulationsstörung • CPP: Eine Verminderung des kraniellen Perfusionsdrucks über einen gewissen Zeitraum kann zu intrakraniellen Perfusionsstörungen und folgend zu irreversiblen, hypoxämischen Schädigungen des empfindlichen Nervengewebes kommen • Serumnatrium: eine pathologische Erhöhung oder Erniedrigung des Serumnatriumwertes kann auf einen zentralen Diabetes insipidus hindeuten • Eine Veränderung des Serumnatriums > 10 mmol/l innerhalb von 24 Stunden kann auf einen zentralen Diabetes insipidus hindeuten

Außerdem müssen in der Anwendung ausschließlich Email-Adressen der zuständigen Transplantationsbeauftragten hinterlegt werden.

Verfahren zur Sicherung der Datensparsamkeit

Damit die per Email verschickten Daten keinen direkten Rückschluss auf den Patienten zulassen, sondern erst mittels der Fallnummer über das klinikinterne Patientendatenmanagementsystem bzw. Krankenhausinformationssystem die Zuordnung zum Patienten hergestellt werden kann, dürfen Vor- und Nachname des Patienten nicht angezeigt werden. Hierzu stehen zwei Optionen zur Verfügung: Erstens, bei der Inbetriebnahme wird die entsprechende Konfiguration vorgenommen, sodass der Name des Patienten stets verschleiert in der Email steht. Die archivierten Originaldateien sind hiervon nicht betroffen. Zweitens, innerhalb der Datenbereitstellung des PDMS zur Software werden Vor- und Nachname des Patienten nicht ausgeleitet.

Außerdem kann durch die Klinik eine minimale Datenausleitung realisiert werden, d.h. nur die oben beschriebenen erforderlichen Daten werden der Anwendung bereitgestellt. Somit werden in der versendeten Email lediglich erforderliche Daten angezeigt.

Beschreibung der Speicherorte und der Datenlöschung

Die Konfiguration der Anwendung, das heißt das Austauschverzeichnis, das Abfrageintervall der Dateien, die Emailadresse der Transplantationsbeauftragten, etwaige CC und BCC Adressen und ob ein Emailversand stattfinden soll, wird in einer SQLite-Datenbank gespeichert.

Zur Speicherung der Dateien, also der Jahresübersicht der kritischen Fälle sowie der archivierten Originaldateien, wird ein sogenanntes docker-volume verwendet. Hierdurch wird auf dem Hostsystem, dem Klinikserver auf dem die Anwendung betrieben wird, ein geschütztes Verzeichnis angelegt und die Daten abgelegt. Dadurch kann die Anwendung bei Neustart auf die gleichen Daten zugreifen.

Es gibt mehrere Möglichkeiten, die Daten innerhalb der Anwendung zu entfernen.

1. Global über den Betriebsserver: Hierbei wird mittels eines Befehls der *Anwendungsadministrierenden* die gesamte Anwendung heruntergefahren sowie die zugehörigen, gespeicherten Daten gelöscht (docker-compose down -v).
2. Manuell über die Benutzeroberfläche: Den *Anwendungsadministrierenden* der Anwendung steht die Option zur Verfügung, die Daten händisch aus der Anwendung zu entfernen. Hierfür nutzen sie die Benutzeroberfläche.
3. Automatisierte Löschung der archivierten Dateien: Die archivierten Dateien, d.h. die Dateien, welche die erfassten Daten zu den Patienten erhalten, werden automatisiert gelöscht. Hierfür ist standardmäßig ein Zeitintervall von 30 Tagen vorgesehen. Das Zeitintervall kann jedoch beim Hochfahren der Anwendung konfiguriert werden, sodass längere und kürzere Löschintervalle ebenfalls möglich sind.

Abkürzungsverzeichnis

Kürzel	**Bedeutung**
IHA	irreversiblen Hirnfunktionsausfall
abTXB	Anwendungsbetreuende Transplantationsbeauftragte
zsTXB	Zuständige Transplantationsbeauftragte
GCS	Glasgow Coma Score
RASS	Richmond Agitation-Sedation Scale
ICP	Intrakranieller Druck

CPP	Zerebralen Perfusionsdruck
PDMS	Patientendatenmanagementsystem
KIS	Krankenhausinformationssystem
TLS	Transport Layer Security
REST	Representational State Transfer
API	Application Programming Interface
MLLP	Minimum Lower Layer Protocol

Quellenverzeichnis

(1) Schulte et al. - Organ donor potential increases despite rising numbers of decompressive craniectomies; Dtsch Arztebl Int 2020; 117: 542-3.

(2) Trabitzsch, Pleul, Barlinn et al. - Automatisiertes elektronisches Screeningtool (DETECT) zur Erkennung des potentiell irreversiblen Hirnfunktionsausfalls Dtsch Arztebl Int 2021; 118: 683-90; DOI: 10.3238/arztebl.m2021.0307

Dokumentenhistorie

Version	Erstellt am	Erstellt durch	Geprüft am	Geprüft durch	Kommentar	Dokument
1.0	14.09.2021	Sepp Höhne	20.09.2021 06.10.2021	Martin Sedlmayr (Leiter ZMI) Christiane Lotzkat (Datenschutzbeauftragte Uniklinikum Carl Gustav Carus Dresden)		DatenschutzkonzeptDETECTv1.0.pdf
2.0	16.12.2021	Sepp Höhne	16.02.2022 18.03.2022	Konrad Pleul / Anne Trabitzsch Krankenhausgesellschaft Sachsen e.V.	Die Anbindung anderer PDM-Systeme macht die Entwicklung einer weiteren Schnittstelle (HL7v2) notwendig.	Statement-DETECT_Datenschutzkonzept_khg-sachsen.pdf
3.0	22.06.2023	Sepp Höhne	27.09.2023	Konrad Pleul	Ergänzung einer Beschreibung des Datenflusses über REST-Schnittstelle Ergänzung das Caches von bereits gemeldeten, kritischen Fällen	