

# Technisches IT-Konzept

## Anhang zum Projektprotokoll Vers. 5.3



### Projektleiter:

Prof. Dr. med. Frank M. Brunkhorst  
Leiter Paul-Martini-Forscherguppe  
für Klinische Sepsisforschung  
Klinik für Anästhesiologie und Intensivtherapie  
Erlanger Allee 101  
07747 Jena



Gefördert vom Bundesministerium für Gesundheit  
Förderkennzeichen: IIA5-2512FSB114



**Version 4.3**

# 1. Inhaltsverzeichnis

1.	Inhaltsverzeichnis .....	2
2.	Abbildungsverzeichnis .....	3
3.	Glossar .....	3
4.	Systemkomponenten .....	4
5.	Einleitung .....	5
6.	Technische Systeme .....	6
6.1.	Datenübertragung Labor zu MDDS (VPN) .....	6
6.2.	Zentrale Datenverarbeitende Systeme .....	6
7.	Authentifizierung und Rollen .....	8
7.1.	Authentifizierung .....	8
7.2.	Administrator Labore (Extern) .....	9
7.3.	Kommunikationsdienstleister (Extern) .....	9
7.4.	Administratoren/IT-Verantwortliche (Intern) .....	10
7.5.	Stammdatenpflege/AlertsNet-Arbeitsgruppe (Intern) .....	10
7.6.	Nutzerpflege/AlertsNet-Arbeitsgruppe (Intern) .....	10
7.7.	Dokumentare externer Versorgungseinrichtungen / klinischer Einrichtungen (Extern) .....	10
7.8.	Berichtsempfänger externer Versorgungseinrichtungen/klinischer Einrichtungen (Extern) .....	11
8.	Administrative Prozesse .....	11
8.1.	Nutzerpflege .....	11
8.2.	Stammdatenpflege .....	11
8.3.	Systempflege .....	12
8.4.	Administration der unterliegenden Systeme .....	12
8.5.	Datenexport .....	12
8.6.	Laboranbindung .....	13
9.	Blutkulturbefund-Verarbeitung .....	13
9.1.	Befundimport .....	13
9.2.	Identifikation von Positivkulturen .....	17
10.	Benachrichtigung der Versorgungseinrichtung .....	17
11.	Kommunikation zwischen Microbiological Data Document System (MDDS) & Clinical Data Document System (CDDS) .....	18
11.1.	eCRF-Eingabe .....	18
12.	Technische Dokumentation .....	20
12.1.	Mengengerüst .....	20
12.2.	Datenauswertung .....	20
12.3.	Datenhaltung .....	20
12.4.	Daten im MDDS: .....	21
12.5.	Daten im CDDS: .....	21
12.6.	Backup .....	36
13.	Anhang .....	36

## 2. Abbildungsverzeichnis

<b>Abbildung 1:</b> Import-Prozess für BK-Befunddaten.....	16
<b>Abbildung 2:</b> Prozess der Dokumentation patientenbezogener klinischer Daten zu relevant-positiv getesteten BK-Befunden.....	19

## 3. Glossar

Begriff	Beschreibung
Befund / Befundnachricht	Strukturierte elektronische Nachricht eines BK-Befundes
BK	Blutkultur
CDDS	Clinical Data Document System
eCRF	electronic Case Report Form (Online-Fragebogen)
CSCC	Center for Sepsis Control and Care (Einrichtung des UKJ)
DES	Data Encryption Standard
FTP	File Transfer Protokoll (Protokoll zur Übermittlung von Dateien)
Hash	Eindeutige Prüfsumme
HL7	Datenkommunikationsstandard im Gesundheitsbereich
HTTPS	Protokoll zur SSL-verschlüsselten Übermittlung von Webseiten
ICD	Amtliche Klassifikation zur Verschlüsselung von Diagnosen in der ambulanten und stationären Versorgung in Deutschland
Labor	Mikrobiologisches Labor für menschliche Blutkulturen
MDDS	Microbiological Data Document System
OPS	Amtliche Klassifikation zum Verschlüsseln von Operationen, Prozeduren und allgemein medizinischen Maßnahmen im stationären Bereich und beim ambulanten Operieren
Primary Key	Eindeutiger Datensatzidentifikator innerhalb einer Tabelle
SFTP	SSL-verschlüsseltes FTP
SIC	Subject Identifier Code (Identifikator für einen zu dokumentierenden Infektionsfall im CDDS)
SSH	Secure Shell (verschlüsselter Wartungszugang zu den Servern)
SSL	Secure Sockets Layer (verschlüsselter Kommunikationskanal)
Versorgungseinrichtung	Medizinische Versorgungseinrichtung für Patienten, z.B. Krankenhaus
VPN	Virtual Private Network (verschlüsselter Kommunikationskanal, Gegenstellen müssen einander bekannt sein, Verbindung muss aktiv initiiert werden per Username/Passwort o.ä.)

## 4. Systemkomponenten

<b>Begriff</b>	<b>Beschreibung</b>
MDDS-Server/	Verarbeitet BK-Befunde
CDDS-Server	Server zur Eingabe zusätzlicher Behandlungsdaten

## 5. Einleitung

Das Ziel des Projekts AlertsNet ist die Verbesserung der Qualitätssicherung in Hinblick auf eine indikationsgerechte und ausreichende Blutkulturdiagnostik. Die erste dreijährige Projektphase wurde als BMG-gefördertes Projekt am 30.09.2011 beantragt und zum 01.04.2012 bewilligt.

Die Durchführung des Projekts setzt eine umfangreiche IT-Struktur voraus. Diese umfasst die Erhebung von Blutkulturbefunden aus mikrobiologischen Laboren, die Verarbeitung der Daten zur Ermittlung von klinisch relevant-positiven Befunden, die Erfassung patientenbezogener Daten klinisch relevant-positiv getesteter Patienten in den teilnehmenden Versorgungseinrichtungen sowie die Bereitstellung der anonymisierten, komplettierten Datensätze zur epidemiologisch-wissenschaftlichen Auswertung. Die Auswertung selbst und die Rückmeldung der Erkenntnisse an die teilnehmenden Partner ist nicht Teil dieses IT-Konzeptes.

Im Auftrag der beteiligten Versorgungseinrichtungen stellen die beteiligten mikrobiologischen Labore elektronisch verarbeitbare Blutkultur-Befunde bereit. Diese werden gespeichert und klassifiziert. Aufgrund der vergebenen Klassifikation wird festgelegt, ob eine Nachdokumentation erfolgen soll. Trifft dies zu, so wird die betroffene Versorgungseinrichtung über die benötigte Nachdokumentation unter Nennung des Patienten und einer unabhängigen Befund-ID (SIC) informiert. Im anderen Fall wird der Datensatz anonymisiert. Die Nachdokumentation erfolgt in einem zusätzlichen aus dem Internet erreichbaren System.

Die Architektur besteht aus einer Kombination aus einer im öffentlichen Bereich per HTTPS gesicherten Dateneingabemaske und einer nicht öffentlich zugänglichen, temporär pseudonymisierten und im Endeffekt immer anonymisierten Blutkulturdatenbank. Die Übertragung von personenbezogenen Daten an die Versorgungseinrichtungen findet dabei ausschließlich per Telefax statt.

Das vorliegende Technische IT-Konzept ergänzt das Projektprotokoll (Kapitel 8 „Datenerhebung“) um technische Informationen. Allgemeine Angaben zum IT-Konzept finden sich dort unter Kapitel 8.1 ff.

## 6. Technische Systeme

### 6.1. Datenübertragung Labor zu MDDS (VPN)

- **VPN-Gateway (Laborseitig)**

- i. Funktion: Stellt verschlüsselten Kommunikationskanal für BK-Nachrichten beim Labordienstleister bereit
- ii. Standort: beim Labordienstleister
- iii. System VPN: VPN-Gateway (Box-Hardware), bereitgestellt durch Kommunikationsdienstleister
- iv. Zugriffsberechtigung: Rolle Kommunikationsdienstleister (VPN-KommDL)
- v. Monitoring: VPN-KommDL  
Alternative: Ist der Datenabruf durch das MDDS nicht möglich erfolgt eine Meldung an VPN-KommDL und den Labordienstleister
- vi. Verschlüsselung des Kommunikationskanals gemäß geltender Standards

- **Quellenanbindung MDDS-Server**

- i. Kommunikation: Initiiert Verbindung zum Bereitstellungsverzeichnis für Befunddateien beim Labordienstleister;  
der Aufbau der VPN- Verbindung erfolgt transparent

### 6.2. Zentrale Datenverarbeitende Systeme

- **MDDS-Server**

- i. Funktion: Verarbeitung der Blutkulturbefund-Dateien  
Zentrale Datenhaltung  
Bewertung der Blutkulturbefunde  
Anonymisierung  
Verwaltung der Faxliste  
  
Identifizierende Daten werden symmetrisch durch Applikation verschlüsselt und nur so gespeichert

- ii. Kommunikation: ***Quellenanbindung an Laborsysteme siehe 5.1***  
Initiiert Verbindung zu CDDS
  - iii. Standort: AlertsNet-DMZ am **UKJ**
  - iv. Zugriffsberechtigung: Rolle Administratoren, Rolle Stammdatenpflege, Rolle Nutzerpflege (jeweils mit entsprechenden Rechten)
  - v. Betrieb: IT-Gruppe des CSCC
  - vi. System: virtuelle Maschine auf Appliance des AlertsNet in eigener DMZ (Apache, Tomcat, Vaadin, PostgreSQL, CentOS 6.x)  
Zugang: VPN mit Token. Applikation ist zusätzlich mit Nutzernamen und Passwort abgesichert
  - vii. Monitoring: IT-Gruppe des CSCC
  - viii. Backup: Auf NAS in AlertsNet-DMZ (täglich mit wöchentlichem Rollover) (Annahme 4 GB)
- **Faxsystem**
    - i. Funktion: Versand der wöchentlich erstellten SIC-Klarnamen-Liste; Faxnummer aus Stammdaten
    - ii. Kommunikation: Fax (Anmerkung: es wird keine Rückmeldung über einen erfolgreichen Versand benötigt)
    - iii. Standort: **UKJ**
    - iv. Zugriffsberechtigungen: Rolle UKJ-Administratoren
    - v. Betrieb: UKJ-Rechenzentrum
    - vi. System: Thor-Gateway (via ukj-Mail-Gateway mit Adressat 0<FaxNr>@fax.med.uni-jena.de)
    - vii. Monitoring: UKJ-Rechenzentrum
- **CDDS**
    - viii. Funktion: Bereitstellung des Nachdokumentationsbogens
    - ix. Kommunikation: HTTPS
    - x. Standort: **UKJ** Forschungsnetz
    - xi. Adresse: <https://crf.alertsnet.org>  
Routing: Port 443 auf Tomcat
    - xii. System: virtuelle Maschine auf Appliance des CSCC im Forschungsnetz (Apache, Tomcat, Vaadin, PostgreSQL, CentOS 6.x)

- xiii. Zugriffsberechtigung: Rolle Administratoren, Rolle  
Dokumentare externe Versorgungseinrichtung
- xiv. Betrieb: IT-Gruppe des CSCC
- xv. Monitoring: IT-Gruppe des CSCC
- xvi. Backup: TiNa ins URZ (täglich mit wöchentlichem Rollover)  
Annahme 1GB

- **externe Dokumentationsplätze**

- i. Funktion: Klinische Dokumentation für klinisch relevant-positive BK-Befunde
- ii. Kommunikation: HTTPS
- iii. Standort: in teilnehmender Versorgungseinrichtung (Desktop-PC)
- iv. System: Internetfähiger PC mit Standard-WebClient
- v. Zugriffsberechtigung: Rolle Dokumentare externe Versorgungseinrichtung
- vi. Betrieb: externe Einrichtung
- vii. Monitoring: externe Einrichtung
- viii. Backup: einrichtungsspezifisch

## **7. Authentifizierung und Rollen**

Da das MDDS wie auch anhängig das CDDS über ein ausgereiftes Rechte- und Rollensystem verfügt und diese zudem dediziert zu vergeben sind (Create-Read-Update-Delete), ist eine spezifische Freigabe von Funktionen über Datenbank- und Betriebssystemebene hinaus innerhalb der Anwendung möglich.

Die Administration des Gesamtsystems (MDDS, CDDS) erfolgt innerhalb des MDDS. Änderungen, die im CDDS erforderlich sind, werden per Webservice unidirektional übertragen.

### **7.1. Authentifizierung**

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:



- Jeder Nutzer erhält ein personalisiertes Login. Die Rechte werden über ein Rollenkonzept vergeben.
- Die Nutzer authentifizieren sich per Passwort. Das Passwort besteht aus mindestens 8 Zeichen. Es muss Groß- und Kleinbuchstaben sowie mindestens 1 Sonderzeichen aus den folgenden enthalten: \$%&!@+\*#[]()\_-:.,; Der Nutzer muss das übermittelte Passwort bei Erstanmeldung ändern.
- Bei Fehleingabe verdoppelt sich die Wartezeit bis zum nächsten Loginversuch ausgehend von 10 Sekunden (10, 20, 40, 80, 160,... Sekunden).
- Das Passwort muss regelmäßig durch den Nutzer gewechselt werden, spätestens jedoch alle 90 Tage. Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht. Die Vergabe eines neuen Passworts ist auch durch den Administrator möglich.
- Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Passwortgestaltung soll gem. den Empfehlungen des IT-Grundschutzkatalogs des BSI Kap. M2.11 vorgenommen werden  
(s. [https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/\\_content/m/m02/m02011.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html)).

## **7.2. Administrator Labore (Extern)**

Die Geschäftsführung der externen mikrobiologischen Labore bestimmen die dortigen Systemadministratoren als Ansprechpartner hinsichtlich der Bereitstellung der mikrobiologischen Blutkulturbefundnachrichten sowie der Struktur der Nachrichten. Die Administratoren müssen sicherstellen, dass die Blutkulturbefunde im vereinbarten Format bereitgestellt werden und die Kommunikationsstrecke laborseitig verfügbar ist.

## **7.3. Kommunikationsdienstleister (Extern)**

Der Kommunikationsdienstleister, der in den Laboren die projektspezifische Appliance zum Versand/Abruf der Labor-Befunde installiert. Mit den Laboren sind Verfahren zur Funktionsprüfung und der Wartung zu vereinbaren.

#### **7.4. Administratoren/IT-Verantwortliche (Intern)**

Administratoren haben vollen Zugriff auf das MDDS wie auch das CDDS. Neben dem Zugriff auf beide Betriebssysteme unter dem „root“ Account besteht auch voller Zugriff auf die Datenbank und die Applicationserver, in denen die AlertsNet-BK-Anwendung (auf dem MDDS) bzw. die eCRF-Anwendung (auf dem CDDS) läuft. Innerhalb der AlertsNet-Anwendung des MDDS-Servers besteht ebenfalls voller Zugriff auf alle relevanten Systembestandteile (Benutzerverwaltung, Gruppenverwaltung, eCRF-Verwaltung, Stammdatenverwaltung (Name, Vorname, Geburtsdatum, Geschlecht), Mappingpflege Keime, Mappingpflege Antiinfektiva). Bei Remoteverbindungen (SSH, SFTP) erfolgt die Authentifizierung auf den Server per Zertifikat, die Authentifizierung auf der Web-Anwendung erfolgt per Nutzernamen und Passwort. Die Kommunikation zwischen Server und Administrations-Rechner wird per VPN und Token gesichert.

#### **7.5. Stammdatenpflege/AlertsNet-Arbeitsgruppe (Intern)**

Die Rolle „Stammdatenpflege“ ermöglicht eingeschränkten Zugriff auf die Stammdatenpflege des MDDSs. Aufgrund des Rechte und Rollensystems ist eine Vergabe dieser Rechte problemlos möglich. Die Stammdatenpflege umfasst die Verwaltung von Stationstypen, Einrichtungstypen, Einrichtungen, Stationen, Laboren und die Anpassung der Mappings für Keime und Antiinfektiva.

#### **7.6. Nutzerpflege/AlertsNet-Arbeitsgruppe (Intern)**

Um im laufenden Betrieb die Rolle „Administratoren“ (siehe 7.4.) nicht übermäßig zu strapazieren ist es erforderlich, bestimmten Personenkreisen innerhalb der Rolle „Nutzerpflege“ das Anlegen von Benutzern zu ermöglichen, die im CDDS dokumentieren können. Innerhalb der Rolle ist es nur möglich Dokumentare und Berichtsempfänger (siehe 7.7. und 7.8.) anzulegen. Andere Funktionen bzw. Rechte sind nicht erforderlich.

#### **7.7. Dokumentare externer Versorgungseinrichtungen / klinischer Einrichtungen (Extern)**

Die Dokumentare in den externen Versorgungseinrichtungen müssen sich mit einem Webbrowser am CDDS anmelden können, um die in der Faxnachricht angegebenen Befunde mit klinischen Daten des Patienten zu dokumentieren. Nur die der Einrichtung zugehörigen

Befunde sind sichtbar. Funktionen, die über das Ausfüllen der Nachdokumentation hinausgehen, sind nicht erforderlich.

#### **7.8. Berichtsempfänger externer Versorgungseinrichtungen/klinischer Einrichtungen (Extern)**

Die Berichtsempfänger in den externen Versorgungseinrichtungen müssen sich mit einem Webbrowser am CDDS anmelden können, um die zusammenfassenden Berichte zur Datenlage (anonymisierte Daten) ihrer jeweiligen Einrichtung abrufen zu können. Nur die der Einrichtung zugehörigen Berichte sind abrufbar.

## **8. Administrative Prozesse**

Folgende Prozesse sind für den Betrieb des AlertsNet-Softwaresystems erforderlich.

### **8.1. Nutzerpflege**

Das Anlegen von neuen Benutzern im MDDS wie auch im CDDS ist eine zentrale und oft wiederkehrende Aufgabe. Jede Funktion des CDDS wie auch des MDDS kann einer Gruppe zugeordnet werden. Die Funktionen sind zudem mit einer Rechematrix versehen. Somit ist es möglich, feingranuliert Anwendungsrechte zu vergeben. Bestimmte Administrator-Rollen (siehe 7.4., 7.5., 7.6.) können nur bestimmte Rollen vergeben. Die Nutzerpflege erfolgt ausschließlich im MDDS. Dieses transferiert die externen Benutzer (siehe 7.7., 7.8.) auf das CDDS per Webservice.

### **8.2. Stammdatenpflege**

Die Stammdatenpflege umfasst die größte Anzahl an Funktionen innerhalb des MDDS und CDDS. Beim Anlegen einer Einrichtung (eines Projektpartners) ist in erster Linie die Einrichtung selbst anzulegen und deren Faxnummer zu verifizieren:

1. Ein Mitarbeiter (Dokumentar) wird von der Geschäftsführung der klinischen Einrichtung benannt. Eine Faxnummer wird telefonisch durchgegeben.
2. Eine Unterschriftsvorlage wird an die genannte Faxnummer gesandt.
3. Der benannte Mitarbeiter sendet die Vorlage unterschrieben zurück.
4. Der gezeichnete Rückmeldebogen wird im Projektordner abgelegt.

Zur Stammdatenpflege werden ebenfalls die Pflege der Mappings von Keimen und Antiinfektiva gezählt. Da jede Einrichtung eigene Bezeichnungen und Abkürzungen verwendet, müssen diese auf zentrale Wertetabellen überführt werden, um eine einheitliche Auswertungen zu ermöglichen.

Um eine differenzierte Auswertung zu ermöglichen, werden ebenfalls die Stationen sowie deren Typ (ITS oder Normalstation) der einzelnen Einrichtungen aufgenommen und der jeweiligen Einrichtung zugeordnet. Beim Import der Blutkultur wird diese dann der entsprechenden Station (falls möglich) zugeordnet. Die Einrichtungen werden ebenfalls typisiert (z.B. Reha-Einrichtung, Klinikum, Universitätsklinikum)

Auch die teilnehmenden Labore werden innerhalb der Stammdatenpflege aufgenommen. Beim Import der Blutkultur werden diese entsprechend zugeordnet und dienen der weiteren qualitativen Verbesserung der Auswertungen.

### **8.3. Systempflege**

Innerhalb der Systempflege werden alle systemtechnischen Verwaltungsaufgaben zusammengefasst. Hierzu gehört das Anlegen der entsprechenden Gruppen, die die benötigten Rollen repräsentieren (Rolle Administratoren, Rolle Dokumentare etc.), und die Zuordnung der festgelegten Anwendungsrechte. Änderungen an den Nutzerrechten werden im AuditLog protokolliert. AuditLog und ApplicationserverLog können von den IT-Verantwortlichen (s. Kapitel 7.4) eingesehen werden.

### **8.4. Administration der unterliegenden Systeme**

Das Betriebssystem, CentOS 6.x, muss fortlaufend ohne Zugriff auf Personen-bezogene Daten überwacht und aktualisiert werden, die Logfiles unter /var/log sind regelmäßig zu prüfen. Auch der installierte Applicationserver und der Webserver müssen regelmäßigen Updates unterzogen werden. Die Aktualität der installierten Software-Pakete wird täglich per Nagios gegen ein zentrales Paket-Repository überprüft.

### **8.5. Datenexport**

Für Auswertungen werden die Daten im CSV Format exportiert. Der Datenexport erfolgt unter Verwendung einer SQL-Konsole direkt auf der Datenbank. Nur anonymisierte Daten werden exportiert. Der Datenbankzugriff erfolgt mit einem lesenden Benutzer unter

eingeschränkten Rechten (nur exportrelevante Daten sind sichtbar). Den Export führen nur Systemadministratoren durch.

## **8.6. Laboranbindung**

Jeder neue Teilnehmer muss an die zentrale AlertsNet-Datenbank (MDDS) angebunden werden, um den Import der Blutkulturbefund-Nachrichten zu ermöglichen. Auf Laborseite muss hierbei eine HL7-Freigabe durch die Laboranbieter zur Verfügung gestellt werden. Die Realisierung der Kommunikationsinfrastruktur erfolgt gemäß dem Kommunikationskonzept des Kommunikationsdienstleisters (s. Anhang). Das VPN-Gateway wird in der DMZ platziert. Eine grundsätzliche Funktionsprüfung erfolgt durch den MDDS-Server: Liegen zum erwarteten Zeitpunkt keine Befunddaten von einem Labor vor, werden die Systemadministratoren des MDDS-Servers informiert.

# **9. Blutkulturbefund-Verarbeitung**

## **9.1. Befundimport**

Vor dem Befundimport werden die Blutkulturbefunde (Gesamtlaborbefunde werden beim Laboranbieter vorgefiltert) beim Labor gepullt (abgeholt). Der Import beginnt mit der Filterung nach End-Befunden. Nur End-Befunde werden tatsächlich übernommen. Alle anderen Nachrichten werden sofort verworfen und gelöscht. Innerhalb des Import-Prozesses erfolgt die Zuordnung zu der jeweiligen Einrichtung.

Da nur mikrobiologische Befunddaten von Interesse sind, erfolgt während des Imports die Extraktion der gewünschten mikrobiologischen Befunddaten (s. Tabelle 2). Bei dem Import erfolgt ein Mapping der mikrobiologischen Befunddaten bzw. der Keimbezeichnungen auf die in der Befunddatenbank des MDDS verwendeten Bezeichnungen. Gleiches gilt für die Antiinfektiva (siehe 8.2.). Da eine Patientenzuordnung erforderlich ist, sind innerhalb des Imports der HL7-Nachrichten auch die Klardaten des Patienten zu extrahieren. Diese umfassen Name, Vorname, Geburtsdatum, Geschlecht (Zuordnung zur Versorgungseinrichtung wird bereits durchgeführt). Weitere Daten werden nicht erfasst. Die Klardaten des Patienten werden anonymisiert. Hierzu werden Name, Vorname, Geburtsdatum, Geschlecht herangezogen. Bei Namen und Vornamen erfolgt eine Normierung der Zeichenketten. Anschließend werden die einzelnen Strings (Name, Vorname, Geburtsdatum, Geschlecht) miteinander konkateniert. Der hieraus entstehenden (Gesamt-)String wird dann per SHA-512 Hash-Algorithmus im

java.security-Package verschlüsselt und gespeichert. Anhand des Hash-Anonyms kann eine Nachverfolgung des Patienten realisiert werden, auch wenn dieser eine andere Einrichtung besucht. Eine Wiederherstellung der Stammdaten aus dem Anonym ist mit realistischen Aufwand nicht möglich (s. Projektprotokoll 5.2, Kapitel 8.1.4.). Danach werden die Stammdaten nach folgenden Regeln gelöscht:

- Handelt es sich nicht um einen Positiv-Befund, so erfolgt die sofortige Löschung der Stammdaten.
- Bei Positivbefunden erfolgt die Löschung der Stammdaten nach erfolgreichem Zurücklesen des komplettierten eCRF, spätestens jedoch nach 60 Tagen.
- Sind die Befund-Nachrichten in irgendeiner Weise fehlerhaft, so werden diese in ein einrichtungsbezogenes Fehlerverzeichnis verschoben. Dabei wird die Nachrichten-Datei mit einem symmetrischen Verschlüsselungsalgorithmus (3DES) verschlüsselt. Zusätzlich wird eine E-Mail an den System-Administrator verschickt, die über den Vorfall informiert. Wird nach 60 Tagen nicht eingegriffen und die fehlerhafte Datei überprüft, erfolgt nach 60 Tagen die Löschung der fehlerhaften Datei.
- Ein Löschprotokoll der Klarnamen kann vom Beauftragten für den Datenschutz der betroffenen klinischen Einrichtung angefordert werden. Der Bericht wird auf der Datenbankebene erzeugt und ist durch die Administratoren abrufbar.

Beim Import wird gleichzeitig ein SIC erzeugt. Die SIC ist eine Zahlenfolge bestehend aus jeweils 3 x 3 Digits getrennt mit einem Bindestrich (123-456-789-X). Als Prüfziffern-Algorithmus kommt der Luhn-Algorithmus zum Einsatz. Die SIC wird anhand der laufenden Nummer des einzelnen Befundes (Primary Keys des relationalen Datensatzes in der MDDS-Datenbank) abgeleitet (PK 1003 → 000-001-003-3), wobei die Ziffernfolge von rechts nach links läuft. Primary Keys größer als 999-999-999 beginnen daher wieder mit 000-000-000. Da die Prüfziffer auf dem Luhn-Algorithmus basiert und dieser anwendungsweit bekannt ist, wird die Prüfziffer nicht mitgeführt sondern jeweils generiert und verglichen (Fax bzw. Eingabe).

**Tabelle 2:** Daten, die aus mikrobiologischen Befundnachrichten nach der BK-Analyse vom MDDS extrahiert werden.

<b>Daten</b>	<b>required / optional</b>	<b>Ablageart in Datenbank</b>	<b>Speicherfrist</b>
Patient Name	required	verschlüsselt (nur bei relevanten Befunden)	max 60 Tage
Patient Vorname	required	verschlüsselt (nur bei relevanten Befunden)	max 60 Tage
Patient Geburtsdatum	required	Klartext (nur bei relevanten Befunden)	Dauerhaft
Patient Geschlecht	required	Klartext (nur bei relevanten Befunden)	Dauerhaft
Beauftragende Station	optional	Klartext	Dauerhaft
Fall-Nr des Patienten	optional	verschlüsselt (nur bei relevanten Befunden)	max 60 Tage
Probe Abnahmedatum	optional	Klartext	Dauerhaft
Probe Eingangsdatum	optional	Klartext	Dauerhaft
Probe BK-Typ	optional	Klartext (Lookup-Wert gespeichert)	Dauerhaft
Probe Datum Untersuchungsergebnis	optional	Klartext	Dauerhaft
Probe Befunddatum	required	Klartext	Dauerhaft
Probe Keim(e)	required	Klartext (Lookup-Wert gespeichert)	Dauerhaft
Probe Resistogramme Wirkstoff	required	Klartext (Lookup-Wert gespeichert)	Dauerhaft
Probe Resistogramme Bewertung	required	Klartext (Lookup-Wert gespeichert)	Dauerhaft
Probe Resistogramme Hemmhofgröße	optional	Klartext	Dauerhaft

Abbildung 1 fasst den Import-Prozess für BK-Befunddaten chronologisch zusammen.

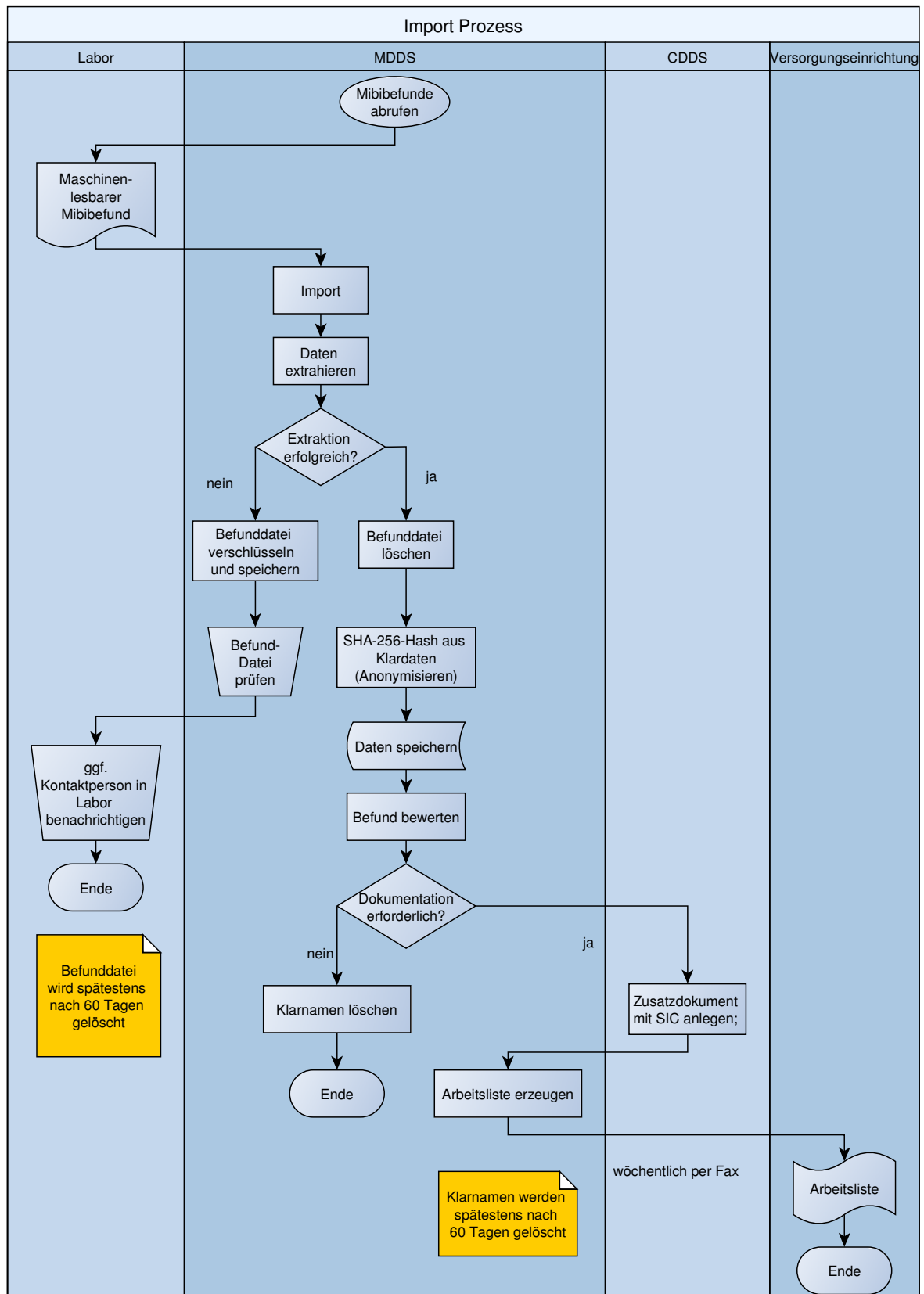


Abbildung 1: Import-Prozess für BK-Befunddaten.



## 9.2. Identifikation von Positivkulturen

Um die mikrobiologischen Daten zu klassifizieren (Positiv-Negativ-Befunde), ist ein entsprechender Algorithmus vorgesehen. Periodisch finden strukturierte Datenbankabfragen statt. Es soll hier patientenbezogen eruiert werden, aus welchen Projekteinrichtungen neue relevante Blutkulturen berichtet wurden.

Selektionskriterien für die Suche je Befund (SIC) und das Auffinden von Positiv-Befunden sind:

1. Erstmaliger Nachweis eines obligat pathogenen Keims. Maßgeblich ist die Keimliste des MDDS-Servers. Die Pflege der Keimliste erfolgt dort. Hierbei ist zu beachten, dass nicht jede Projekteinrichtung gleiche Bezeichnungen der Keime pflegt. Es muss daher pro Einrichtung/Labor eine Mapping-Tabelle gepflegt werden (siehe 8.2.).
2. Erneuter Nachweis ( $n > 1$ ) eines nicht-obligat pathogenen Keims (diese sind entsprechend in der Keimliste markiert - z.B. *Staphylococcus epidermis*) innerhalb von 72 Stunden (definiert über den Zeitpunkt der BK-Abnahme).
3. Der Nachweis eines zusätzlich relevanten Keimnamens bei schon in den letzten 12 Tagen positiv selektierten Patienten (Hintergrund: Bei adäquater Antiinfektivagabe gilt ein Keim nach 12 Tagen als eliminiert.)

## 10. Benachrichtigung der Versorgungseinrichtung

Der Versand der Nachricht über dokumentationspflichtige positive BK-Befunde erfolgt über ein elektronisches Fax. Wöchentlich wird eine Meldeliste erzeugt und versandt, die u.a. Klarnamen, Keime, Fallnummer und die SIC mit zugehörigem Befunddatum (Berichtszeitpunkt) und BK-Abnahmedatum enthält.

Die Kontaktdaten und die Faxnummer werden in der Einrichtungskonfiguration des MDDS per Eingabemaske gepflegt. Die Faxnummern werden monatlich validiert (s. 8.2.).

Die Kommunikation per Fax wurde gewählt, weil es ein etabliertes Verfahren der Informationsübermittlung mit akzeptablen Laufzeiten ist.

Von einer bereits bestehenden Infrastruktur zur verschlüsselten Email-Kommunikation ist in den beteiligten Versorgungseinrichtungen nicht auszugehen.

Eine Kommunikation per Brief würde zu nochmals verlängerten Bearbeitungszeiten und damit längeren Speicherfristen von sensiblen Daten im BK-System führen.

Bei Versenden der Faxnachricht wird nicht auf eine Versand-Bestätigung gewartet. Vielmehr werden für nicht erfolgte Dokumentationen die Daten erneut zum nächsten regulären Zeitpunkt versandt. Werden diese bis zu 60 Tage nach dem erfolgten Import nicht dokumentiert, erfolgt die vollständige Anonymisierung durch Löschen der Klarnamensbestandteile mit einem Vermerk auf die nicht erfolgte Nachdokumentation.

## **11. Kommunikation zwischen Microbiological Data Document System (MDDS) & Clinical Data Document System (CDDS)**

Die Kommunikation zwischen dem MDDS (Client) und dem CDDS (Server) erfolgt unidirektional, d.h. das MDDS ruft an und holt Daten ab. Durch eine entsprechende Firewall-Konfiguration ist es dem CDDS nicht möglich, Verbindungen zum MDDS aufzunehmen. Identifiziert das MDDS einen relevanten Befund, so wird im CDDS (vom MDDS getriggert) ein leerer eCRF mit entsprechender SIC per Webservice angelegt.

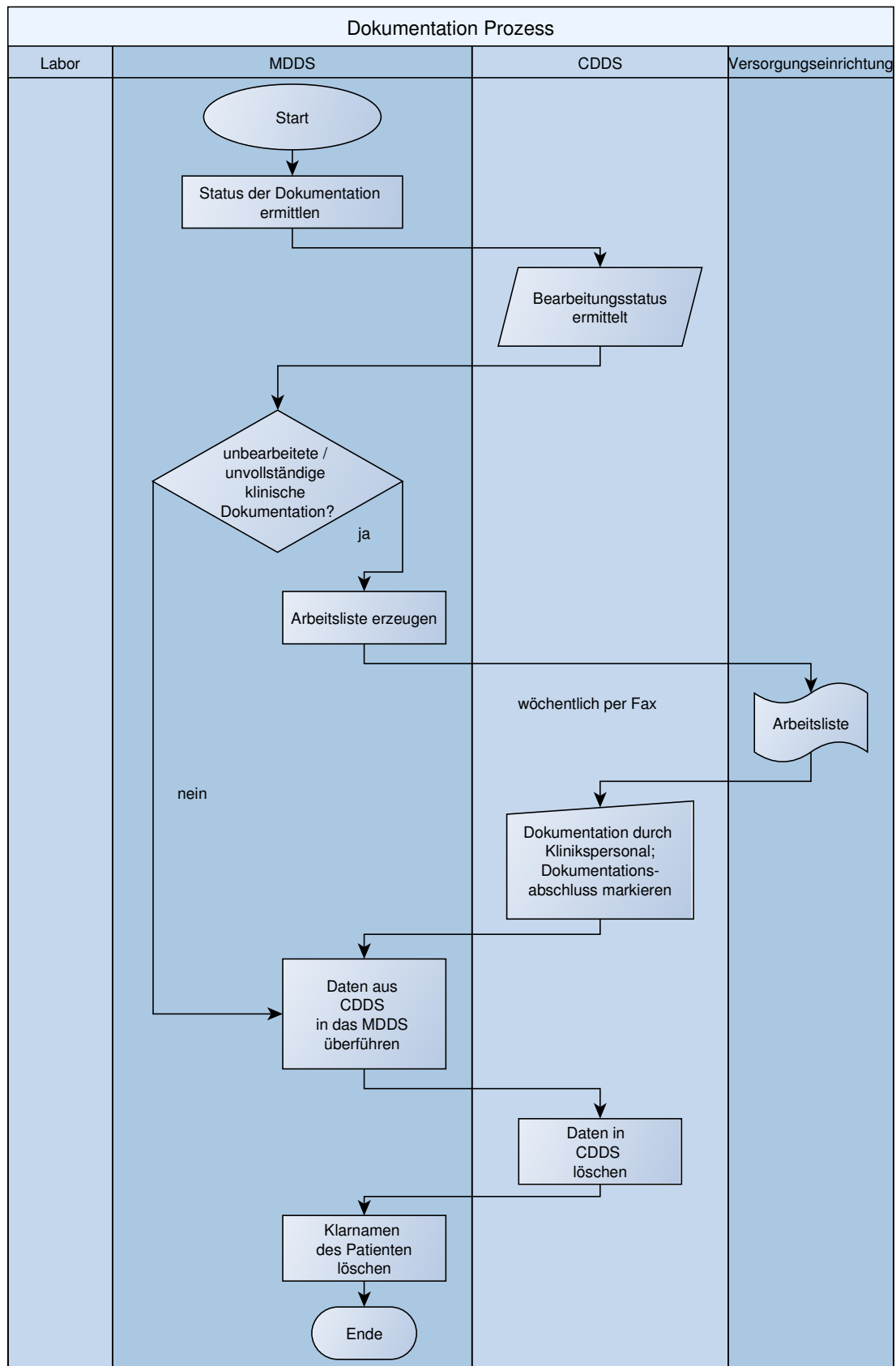
### **11.1. eCRF-Eingabe**

In den Versorgungseinrichtungen (Projekteinrichtungen) erfolgt die ergänzende Dokumentation von Positivbefunden mittels eines Screening-Fragebogens. Der Fragebogen wird dabei im eigenentwickelten CDDS abgebildet.

Der Dokumentar kommuniziert per Webbrowser via HTTPS mit dem CDDS. Er muss sich mit Nutzernamen und Passwort am System authentifizieren. Anhand der Klarnamen-SIC-Liste kann der Dokumentar anschließend mit Hilfe den angelegten eCRF ausfüllen. Die angezeigte SIC-Liste ist einrichtungsabhängig; jede Einrichtung sieht nur ihre eigenen Fälle.

Abbildung 2 fasst den Prozess der Dokumentation klinischer Daten von Patienten, deren BKs

einen klinisch relevant-positiven Befund aufzeigen, zusammen.



**Abbildung 2:** Prozess der Dokumentation patientenbezogener klinischer Daten zu relevant-positiv getesteten BK-Befunden.

## 12. Technische Dokumentation

### 12.1. Mengengerüst

Bettentage / 1.000 Patienten (85% mittlere Auslastung)	6.330
BK-Befunde pro Jahr (Anzahl BK-Sets pos. & neg. x 50; ~50 BK-Sets / 1.000 Patiententage)	316.501
Zahl positive BK-Sets x 8% (Positivitätsrate)	25.320
Zahl klinisch relevanter positiver BK-Sets x 80% (~20% Kontaminationsrate)	20.256
Patienten mit klinisch relevanten positiven BK-Sets (x 25%)	5.064
Anzahl erwartete klinisch relevanter Positivbefunde pro Woche	ca. 390
Anzahl teilnehmender Labore (Primärdatenlieferanten):	17-19
Anzahl teilnehmender Versorgungseinrichtungen:	ca. 40
Zu versendende Faxmeldungen pro Woche	ca. 40

### 12.2. Datenauswertung

Die Datenauswertung ist nicht Teil des IT-Konzepts. Die Auswertung erfolgt durch die Arbeitsgruppe Epidemiologie und Statistik (siehe auch AlertsNet-Studienprotokoll). Die Daten werden den Projektpartnern als anonymisierter Export zur Verfügung gestellt.

Zukünftig ist ein Online-Feedback innerhalb des Screening-Systems denkbar.

### 12.3. Datenhaltung

In der zentralen Befunddatenbank des MDDS-Servers ist eine vollständige Datenhaltung erforderlich. Im CDDS (das extern zugreifbar ist) werden nur Untermengen der Daten (zu bearbeitende CRFs) gehalten.

Der MDDS-Server speichert für maximal 60 Tage die Klarnamen in verschlüsselter Form.

Im CDDS sind nur anonymisierte Daten und die Daten zur Struktur der Einrichtung (Stationen) gespeichert.

**12.4. Daten im MDDS:**

1. Administrativen Daten, Patienten, Blutkulturbefunde, Kontakte zu den Häusern, Stationen, Benutzer und Rechtemanagement, Mappings von Antiinfektiva und Keimen, Medikamente.
2. Patienten mit Positivbefunden werden maximal 60 Tage mit verschlüsselten Klarnamen gespeichert. Erfolgt keine Nachdokumentation in dieser Zeit, werden die Klarnamen gelöscht. Ist die Nachdokumentation vollständig erfolgt, werden die Klarnamen sofort gelöscht.
3. Klarnamen werden immer TrippleDeS verschlüsselt gespeichert.
4. Patienten werden per SHA512-Hash über Vorname, Nachname, Geburtsdatum und Geschlecht anonymisiert, Klarnamen werden gemäß 2. gelöscht.
5. Klarnamen von Patienten ohne Positivbefunde werden sofort gelöscht.

**12.5. Daten im CDDS:**

1. Benutzer und Rechtemanagement, normierte Blutkulturbefunde, Patientenanonym ,Geburtsjahr und Geschlecht, Einrichtungen und Stationen, Medikamente.
2. eCRF in vollständiger Ausprägung bis zur Abholung durch das Blutkultur-System.

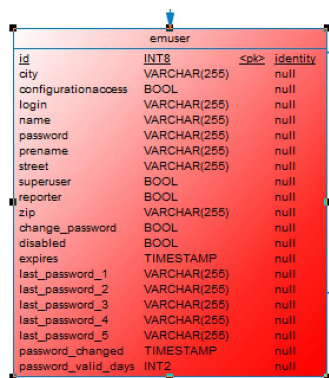
Folgende Daten werden in der Datenbank gehalten:

**Benutzer**

Bezeichnung	Datentyp	Bemerkung
Id	Int8	Identifizier
City	Varchar	
configurationaccess	Boolean	Zugriff auf die Konfigurationsfunktionen gestattet z.B. Pflege von Mappings, Einrichtungen, Nutzer
Login	Varchar	
Password	Varchar	
Name	Varchar	
Prenome	Varchar	
Street	Varchar	
Superuser	Boolean	Systempflege, Zugriff auf alle Funktionen
Reporter	Boolean	Report-Administrator
Zip	Varchar	
Change_Password	Boolean	bei aktiv Änderung Passwort bei nächstem Login
disabled	Boolean	Login abgeschaltet

expires	Timestamp	Ablaufdatum
Last_password_1	Varchar	Passwörter (Hash), die nicht mehr verwendet werden dürfen (die letzten fünf)
Last_password_2	Varchar	
Last_password_3	Varchar	
Last_password_4	Varchar	
Last_password_5	Varchar	
Password_Changed	Timestamp	Letzte Änderung des Passwortes
Password_valid_days	Int2	Nach wieviel Tagen muss das Passwort geändert werden

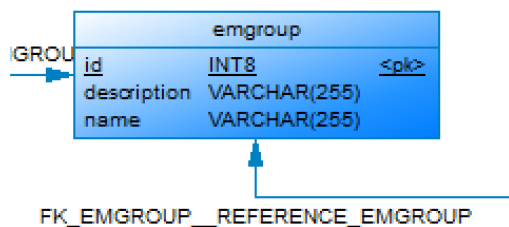
Tabelle im Datenmodell



## Gruppe

Id	Int8	Identifizier
Name	Varchar	
Description	Varchar	Null erlaubt

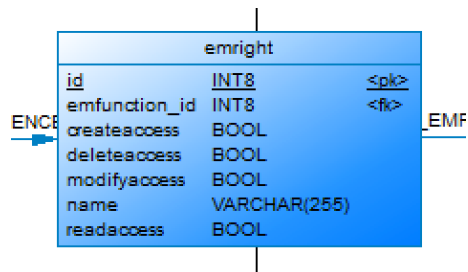
Tabelle im Datenmodell



**Recht**

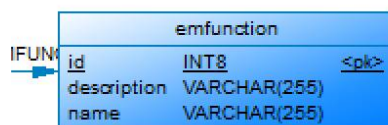
Id	Int8	Identifizier
emfunction_id	Int8	Referenz auf entsprechende Anwendungs-Funktion z.B. Verwaltung Benutzer
createaccess	Boolean	
deleteaccess	Boolean	
modifyaccess	Boolean	
Name	Varchar	Bezeichnung der Funktion der Anwendung
readaccess	Boolean	

Tabelle im Datenmodell

**Funktion**

Id	Int8	
Description	Varchar	Beschreibung
Name	Varchar	

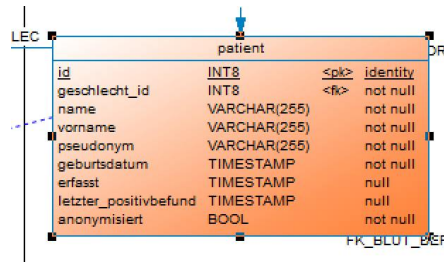
Tabelle im Datenmodell

**Patient**

id	Int8	Identifizier
Geschlecht_id	Int8	Referenz auf Geschlechter
<b>Name</b>	<b>Varchar</b>	
<b>Vorname</b>	<b>Varchar</b>	
Anonym	Varchar	
Geburtsdatum	Date	
Erfasst	Date	
Letzter_positivbefund	Date	Datum des letzten Positiv-Befund
Anonymisiert	Boolean	Ist der Patient anonymisiert

**Alle Fett dargestellten Informationen werden nach spätestens 60 Tagen gelöscht (Positivbefunde)!**

Tabelle im Datenmodell



### Befund

<b>Id</b>	Int8	Identifizier
Patient_id	Referenz	Referenz Patient
Labor_id	Referenz	Referenz Labor
Einrichtung_id	Referenz	Referenz Einrichtung
Station_id	Referenz	Referenz auf Station
Blut_Befund_Status_id	Referenz	Referent auf den Status der Blutkultur (z.B. neu importiert, nicht relevant etc.)
Blut_Befund_id	Referenz	Bei Zusammenfassung, mit welchem Befund
Algo_Status_id	Referenz	Welcher Status nach Algorithmus (z.B. obligat zusammengefasst etc.)
Crf_id	Referenz	Falls befund positiv, referenz auf CRF
<b>Fallnummer</b>	Varchar	
<b>SIC</b>	Varchar	Identifikator
<b>Behandlung_fokus</b>	Varchar	Fokus der Behandlung (nur Jena), Textfeld vom Arzt ausgefüllt
Probeeingang	Date	
Anforderung	Date	
Anzahl der Keime	int	
positiv	boolean	
<b>Auftragsnummer_extern</b>	Varchar	Externe Auftragsnummer (z.B. Labor)
<b>Auftragsnummer</b>	Varchar	Auftragsnummer der Einrichtung
Material	Varchar	
Abnahmezeitpunkt	Date	
Eingangszeitpunkt	Date	
Berichtszeitpunkt	Date	
Crf_komplett	boolean	eCRF ausgefüllt
anonymisiert	Date	Wann wurde anonymisiert
Beschreibung	Varchar	Beschreibung ggf. Infos aus der Datei



## Tabelle im Datenmodell

blut_befund			
id	INT8	<pk>	identity
patient_id	INT8	<fk1>	not null
labor_id	INT8	<fk2>	null
einrichtung_id	INT8	<fk3>	not null
station_id	INT8	<fk4>	null
blut_befund_status_id	INT8	<fk5>	not null
blut_befund_id	INT8	<fk6>	null
algo_status_id	INT8	<fk7>	null
orf_id	INT8	<fk8>	null
fallnummer	VARCHAR(255)		null
sic	varchar(255)		null
behandlung_fokus	varchar(255)		null
probeeingang	TIMESTAMP		null
anforderung	TIMESTAMP		null
anzahl_keime	INT2		null
positiv	BOOL		null
auftragsnummer_extern	varchar(255)		null
auftragsnummer	varchar(255)		null
material	VARCHAR(255)		null
abnahmezeitpunkt	TIMESTAMP		not null
eingangszeitpunkt	TIMESTAMP		null
berichtszeitpunkt	TIMESTAMP		not null
orf_komplett	BOOL		null
anonymisiert	TIMESTAMP		null
beschreibung	varchar(65536)		null

Aus positiven Blutkulturbefunden werden in der Datenbank folgende Berichtelemente (Items) gespeichert:

- Datum und Zeit des Probeneingangs im Labor (= Eingangsscan, Zeitstempel xx.xx.xxxx yy:yy)
- Wenn im HL7-File enthalten: Anforderungsdatum und -zeit (= Erstellungszeitpunkt des Laborauftrags)
- Wenn im HL7-File enthalten: Abnahmedatum und -zeit der Blutkultur
- Wenn im HL7-File enthalten: ob Blutkultur positiv ist
- Berichtszeitpunkt (= Erstellungszeitpunkt (Datum und Zeit ) des HL7-„Final Report“-Files)
- Patientenvorname, -nachname, Geburtsdatum und Geschlecht  
→ als Grundlage für einen anonymisierten HASH-String
- einsendende Einrichtung inkl. Abbildung der Organisationsstruktur
- Anzahl der nachgewiesenen Keime
- Art der positiven Kultur (Status)
- Speziesbezeichnung (Keimnamen laut “List of Prokaryotic names with Standing in Nomenclature”, <http://www.bacterio.cict.fr/>, ca. 2.500 verschiedene Varianten als Referenz); Übereinstimmungstabellen für die einzelnen Laboranbieter sollen vorgängig basierend auf den Stammdaten der Laboranbieter erstellt werden.

Für Keime, die nicht bekannt sind, ist ein ErrorLog eingerichtet, um die entsprechenden Keime ergänzen zu können.

### Keim

Id	Int8	Identifizier
Bezeichnung	Varchar	
Beschreibung	Varchar	
code	Varchar	
Obligat_patogen	Boolean	
nicht_obligat_patogen	Boolean	
junk	Boolean	

## Tabellen im Datenmodell

keim			
id	INT8	<pk>	identity
bezeichnung	varchar(255)		not null
beschreibung	varchar(255)		null
code	varchar(255)	<ak>	not null
obligat_patogen	BOOL		null
nicht_obligat_patogen	BOOL		null
junk	BOOL		null

Zu „junk“ Keim Mapping würde beispielsweise die Bezeichnung „Schnellresistenz“ aus der Keimliste swisslab Jena gehören.

**Keim Mapping (Laborabhängig)**

Id	Int8	Identifizier
Keim_Id	Int8	Referenz auf Keim
Labor_id	Int8	Referenz auf Labor
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
erstellt	Date	
geändert	Date	

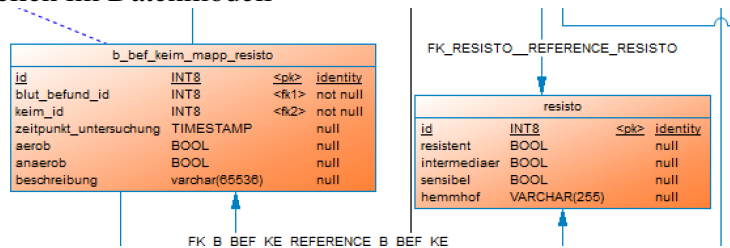
## Tabellen im Datenmodell

kmapp			
id	INT8	<pk>	identity
keim_id	INT8	<fk1>	null
labor_id	INT8	<ak, fk2>	not null
bezeichnung	varchar(255)		not null
beschreibung	varchar(255)		null
code	varchar(255)	<ak>	not null
erstellt	TIMESTAMP		null
geändert	TIMESTAMP		null

**Resistogramm**

<b>Tabelle</b>		
<b>Blut_Befund_keim_mapp_resisto</b>		
Id	Int8	Identifizier
Blut_Befund_id	Referenz	
Keim_id	Referenz	
Zeitpunkt_Untersuchung	Date	
aerob	Boolean	
anaerob	Boolean	
Beschreibung	Varchar	
<b>Tabelle Resisto</b>		
Id	Int8	Identifizier
resistent	Boolean	
intermediaer	Boolean	
sensibel	Boolean	
Hemmhof	Varchar	

## Tabellen im Datenmodell



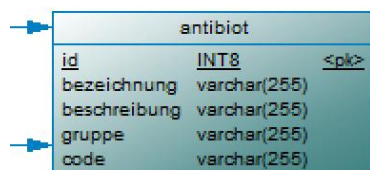
Resistogramm je Keim mit folgenden Subitems:

- Antiinfektivum (englische generische Bezeichnung laut European Pharmacopoeia; ca. 50 mögliche Substanzen)
- Interpretierte Keimempfindlichkeit (S/I/R) je Antiinfektivum
- Wenn in Befundnachricht enthalten: minimale Hemmkonzentration je Antiinfektivum
- Keim

**Antiinfektivum (Einrichtungsunabhängig)**

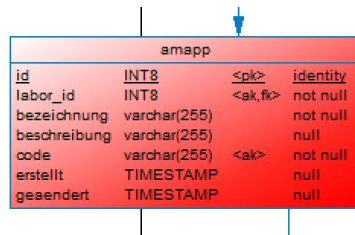
Id	Int8	Identifizier
Bezeichnung	Varchar	
Code	Varchar	
Gruppe	Varchar	
Beschreibung	Varchar	

Tabelle im Datenmodell

**Antiinfektivum Mapping (Einrichtungsabhängig)**

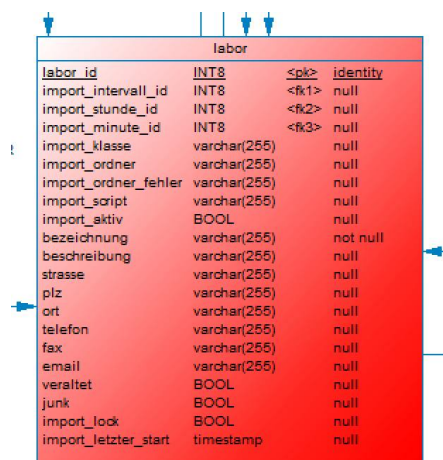
Id	Int8	Identifizier
Labor_id	Referenz	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
erstellt	Date	
geändert	Date	

## Tabelle im Datenmodell

**Labor**

Id	Int8	Identifizier
Import_intervall_id	Referenz	
Import_stunde_id	Referenz	
Import_minute_id	Referenz	
Import_klasse	Varchar	
Import_ordner	Date	
Import_ordner_fehler	Date	
Import_script	Varchar	
Import_aktiv	boolean	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Strasse	Varchar	
PLZ	Varchar	
Ort	Varchar	
Telefon	Varchar	
Fax	Varchar	
eMail	Varchar	
veraltet	boolean	
Junk	boolean	
Import_lock	boolean	
Import_letzter_start	Date	

## Tabelle im Datenmodell



**Einrichtung**

Id	Int8	
Einrichtungstyp_id	Referenz	
Import_intervall_id	Referenz	
Import_stunde_id	Referenz	
Import_minute_id	Referenz	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
Kontakt_Strasse	Varchar	
Kontakt_plz	Varchar	
Kontakt_ort	Varchar	
Kontakt_telefon	Varchar	
Kontakt_fax	Varchar	
Kontakt_email	Varchar	
Kontakt_name	Varchar	
Kontakt_vorname	boolean	
Import_letzter_start	Varchar	
Fax_letzter_start	Date	
Algo_letzter_start	Date	
Import_lock	boolean	
Algo_lock	boolean	
Fax_lock	boolean	
Befund_import_marker	Varchar	

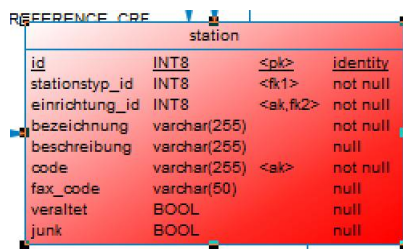
## Tabelle im Datenmodell



**Station**

Id	Int8	
Stationstyp	Referenz	
Einrichtung	Referenz	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
Fax_Code	Varchar	Stationsbezeichnung die auf dem Fax erscheint
veraltet	Boolean	
junk	Boolean	

Tabelle im Datenmodell

**Einrichtungstyp**

Id	Int8	
Name	Varchar	
Bezeichnung	Varchar	
Beschreibung	Varchar	

Tabelle im Datenmodell

**Stationstyp**

Name	Varchar	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	varchar	

## Tabelle im Datenmodell

stationstyp		
id	INT8	<pk>
bezeichnung	varchar(255)	
beschreibung	varchar(255)	
code	varchar(255)	



## eCRF (gemäß eCRF-Umsetzung – siehe hierzu eCRF Form)

Id	Int8	Identifizier
Station_id	Int8	Referenz Station
Einrichtung_id	Int8	Referent Einrichtung
emuser_id	Int8	Referenz User der editiert hat
CRF_entlassung_id	Int8	Referenz Entlassung
CRF_status_id	Int8	Referent Status des CRF (abgeschlossen etc.)
SIC	varchar	Generierte Zeichenfolge des Fax
Version	varchar	Version des CRF
Geburtsdatum	date	aus Blut Befund
		<b>Demografische Daten</b>
dd_geburtsjahr	date	Eingabe in CRF
dd_geschlecht	Int8	
dd_datum_aufnahme_krankenhaus	date	
dd_aufenthalt	Int8	
dd_wohnort	varchar	
dd_plz	varchar	
		<b>Stationen</b>
sta_stationen_48h_unbekannt	boolean	
sta_station_zeitpunkt_unbekannt	boolean	
sta_datum_abnahme_blutkultur	date	
sta_datum_abnahme_unbekannt	boolean	
		<b>Risikofaktoren</b>
rfns_op_30_tage	Int8	
rfns_zentraler_venenkatheter	Int8	
rfns_periphere_venenkanuele	Int8	
rfns_maschinelle_beatmung	Int8	
rfns_harnblasenkatheter	Int8	
		<b>Vermuteter oder wahrscheinlicher Infektionsursprung</b>
vwiu_nosokomial	Int8	
vwiu_ambulant_erworben	Int8	
vwiu_allgemeinstation	Int8	
vwiu_its	Int8	
vwiu_externe_einrichtung	Int8	
vwiu_unbekannt	Int8	



		<b>Infektionslokalisation am Tag der Blutkulturabnahme</b>
itbka_primaere_bakteriaemie	Int8	
itbka_sb_zns	Int8	
itbka_sb_kardiovaskulaer	Int8	
itbka_sb_thorakal	Int8	
itbka_sb_pneumonie	Int8	
itbka_sb_sonstige	Int8	
itbka_sb_intraabdominal	Int8	
itbka_sb_gastrointestinal	Int8	
itbka_sb_urogenital	Int8	
itbka_sb_gefaesskathinfektion	Int8	
itbka_sb_chrg_wundinfektion	Int8	
itbka_sb_knochen_weichteile	Int8	
itbka_sb_andere	Int8	
itbka_sb_unbekannt	Int8	
		<b>Schweregrad</b>
msi_sepsis	Int8	
		<b>Entlassungsdiagnosen</b>
ed_kh_hauptdiagnose	varchar	
ed_kh_hptdgn_beschreibung	varchar	
ed_nd_diabetes	Int8	
ed_nd_kardiovaskulaer	Int8	
ed_nd_cerebrovaskulaer	Int8	
ed_renale_dysfunktion	Int8	
ed_copd	Int8	
ed_leberzirrhose	Int8	
ed_solide_haem_tumor	Int8	
ed_therap_immunsupp	Int8	
		<b>Antimikrobielle Therapie</b>
at_zeitpunkt_bk_abnahme	Int8	
at_nach_bk_abnahme	Int8	
		<b>Nacherhebung</b>
ne_patient_its	Int8	
ne_patient_lebend_entlassen	Int8	
ne_datum_entl_oder_verstb	date	
ne_entl_einrichtung	varchar	
ne_weiter_behandlung	boolean	
		<b>Status</b>
abgeschlossen	boolean	
angelegt	date	
geaendert	date	
		<b>Infektionslokalisation am Tag der Blutkulturabnahme (Ergänzungen)</b>
itbka_unbekannt	Int8	
itbka_tia_pneumonie	Int8	

itbka_tia_bronchitis	Int8	
itbka_tia_pleuraempyem	Int8	
itbka_tia_mediastinitis	Int8	
itbka_tia_andere	Int8	
itbka_tia_nicht_naecher	Int8	
itbka_uri_harnweg	Int8	
itbka_uri_geschlechtsorgane	Int8	
itbka_uri_niere	Int8	
itbka_uri_andere	Int8	
itbka_uri_nicht_naecher	Int8	
itbka_izns_meningitis	Int8	
itbka_izns_andere	Int8	
itbka_izns_nicht_naecher	Int8	
itbka_kgi_spondylodisitis	Int8	
itbka_kgi_osteomyelitis	Int8	
itbka_kgi_gelenkinfektion	Int8	
itbka_kgi_protheseninfektion	Int8	
itbka_kgi_andere	Int8	
itbka_kgi_nicht_naecher	Int8	
itbka_iks_endo_mitralklappe	Int8	
itbka_iks_endo_aortenklappe	Int8	
itbka_iks_andere	Int8	
itbka_iks_nicht_naecher	Int8	
itbka_hno_oropharyngeale	Int8	
itbka_ai_peritonitis	Int8	
itbka_ai_gallenblase_gaenge	Int8	
itbka_ai_leber	Int8	
itbka_ai_pankreas	Int8	
itbka_ai_gastrointestinale_inf	Int8	
itbka_ai_sonst_intra_ge_or	Int8	
itbka_ai_andere	Int8	
itbka_ai_nicht_naecher	Int8	
itbka_hwi_hautinfektion	Int8	
itbka_hwi_weichteilinfektion	Int8	
itbka_hwi_inf_dekubitalulcus	Int8	
itbka_hwi_andere	Int8	
itbka_hwi_nicht_naecher	Int8	
itbka_postop_wundinfektion	Int8	
		<b>Schweregrad (ergänzungen)</b>
msi_sirs	Int8	
msi_organdysfunktion	Int8	
msi_septischer_schock	Int8	

## Tabelle im Datenmodell

cfr			
id	INT8	<pk>	identity
station_id	INT8	<fk1>	null
einrichtung_id	INT8	<fk2>	null
emuser_id	INT8	<fk3>	null
cfr_entlassung_id	INT8	<fk4>	null
cfr_status_id	INT8	<fk5>	null
sic	VARCHAR(255)		null
version	varchar(255)		null
geburtsdatum	TIMESTAMP		not null
dd_geburtsjahr	TIMESTAMP		null
dd_geschlecht	INT2		null
dd_datum_aufnahme_krankenhaus	TIMESTAMP		null
dd_aufenthalt	INT2		null
dd_wohntort	VARCHAR(255)		null
dd_plz	VARCHAR(255)		null
sta_stationen_48h_unbekannt	BOOL		null
sta_station_zeitpunkt_unbekannt	BOOL		null
sta_datum_abnahme_blutkultur	TIMESTAMP		null
sta_datum_abnahme_unbekannt	BOOL		null
rfms_op_30_tage	INT2		null
rfms_zentraler_venenkatheter	INT2		null
rfms_periphere_venenkanuele	INT2		null
rfms_maschinelle_beatmung	INT2		null
rfms_hamblisenkatheter	INT2		null
wwu_nosokomial	INT2		null
wwu_ambulant_erworben	INT2		null
wwu_allgemeinstation	INT2		null
wwu_its	INT2		null
wwu_externer_einrichtung	INT2		null
wwu_unbekannt	INT2		null
itbka_primaere_bakteriaemie	INT2		null
itbka_sb_zns	INT2		null
itbka_sb_kardiovaskulaer	INT2		null
itbka_sb_thorakal	INT2		null
itbka_sb_pneumonie	INT2		null
itbka_sb_sonstige	INT2		null
itbka_sb_intraabdominal	INT2		null
itbka_sb_gastrointestinal	INT2		null
itbka_sb_urogenital	INT2		null
itbka_sb_gefaesskathinfektion	INT2		null
itbka_sb_chrg_wundinfektion	INT2		null
itbka_sb_knochen_weichteile	INT2		null
itbka_sb_andere	INT2		null
itbka_sb_unbekannt	INT2		null
msl_sepsis	INT2		null
ed_kh_hauptdiagnose	VARCHAR(255)		null
ed_kh_hptdgn_beschreibung	VARCHAR(255)		null
ed_nd_diabetes	INT2		null
ed_nd_kardiovaskulaer	INT2		null
ed_nd_cerebrovaskulaer	INT2		null
ed_renale_dysfunktion	INT2		null
ed_copd	INT2		null
ed_leberzirrhose	INT2		null
ed_solide_haem_tumor	INT2		null
ed_therap_immunsupp	INT2		null
at_zeitpunkt_bk_abnahme	INT2		null
at_nach_bk_abnahme	INT2		null
ne_patient_its	INT2		null
ne_patient_lebend_entlassen	INT2		null
ne_datum_entl_oder_verstb	TIMESTAMP		null
ne_entl_einrichtung	VARCHAR(255)		null
ne_weiter_behandlung	BOOL		null
abgeschlossen	BOOL		null
angelegt	TIMESTAMP		null
geaendert	TIMESTAMP		null
itbka_unbekannt	INT2		null
itbka_tia_pneumonie	INT2		null
itbka_tia_bronchitis	INT2		null
itbka_tia_pleuraempyem	INT2		null
itbka_tia_mediastinitis	INT2		null
itbka_tia_andere	INT2		null
itbka_tia_nicht_naehher	INT2		null
itbka_url_hamweg	INT2		null
itbka_url_geschlechtsorgane	INT2		null
itbka_url_niere	INT2		null
itbka_url_andere	INT2		null
itbka_url_nicht_naehher	INT2		null
itbka_izns_meningitis	INT2		null
itbka_izns_andere	INT2		null
itbka_izns_nicht_naehher	INT2		null
itbka_kgl_spondylodiszitis	INT2		null
itbka_kgl_osteomyelitis	INT2		null
itbka_kgl_gelenkinfektion	INT2		null
itbka_kgl_protheseninfektion	INT2		null
itbka_kgl_andere	INT2		null
itbka_kgl_nicht_naehher	INT2		null
itbka_iks_endo_mitralklappe	INT2		null
itbka_iks_endo_aortenklappe	INT2		null
itbka_iks_andere	INT2		null
itbka_iks_nicht_naehher	INT2		null
itbka_hno_propharyngeale	INT2		null
itbka_ai_peritonitis	INT2		null
itbka_ai_gallenblase_gaenge	INT2		null
itbka_ai_leber	INT2		null
itbka_ai_pankreas	INT2		null
itbka_ai_gastrointestinale_inf	INT2		null
itbka_ai_sonst_intra_ge_or	INT2		null
itbka_ai_andere	INT2		null
itbka_ai_nicht_naehher	INT2		null
itbka_hwi_hautinfektion	INT2		null
itbka_hwi_weichteilinfektion	INT2		null
itbka_hwi_inf_dekubitalculus	INT2		null
itbka_hwi_andere	INT2		null
itbka_hwi_nicht_naehher	INT2		null
itbka_postop_wundinfektion	INT2		null
msl_sirs	INT2		null
msl_organdysfunktion	INT2		null
msl_septischer_schock	INT2		null

Bei einer zentralen Pflege der Stationen ist die Ausrichtung bereits vorgegeben. Dies ist zu eruieren. Wird eine Station geändert oder ändert sich die Ausrichtung, so muss diese neu angelegt und die alte Station auf veraltet gesetzt werden.

Die ICD- und OPS-Codes werden nur nach ihrer Struktur geprüft.

## 12.6. Backup

Das Backup der Systeme erfolgt durch den Systembetreiber. Das Backup erfolgt täglich, das Rollover monatlich. Es werden alle datenschutzrechtlichen Gesichtspunkte bei der Backupstrategie berücksichtigt. Das IT-Personal ist in die datenschutzrechtlichen Zusammenhänge eingewiesen. Der Backup-Umfang ist im MDDS und CDDS identisch.

Inhalte des Backup:

- Full-Dump der Datenbanken
  - Verwaltungs-Datenbank Postgres
  - Nutzdatenbank MDDS
- Datei-Backups
  - Verzeichnis /etc (Konfigurationen)
  - Verzeichnis /usr/local (Lokale Programme und Shell-Skripte)
  - Verzeichnis /opt (Programme (Applikationsserver, etc.))
  - Verzeichnis /var/www (Verzeichnis des Webservers)
  - Verzeichnis /var/local (variable Daten im Zusammenhang mit /usr/local)
  - Verzeichnis /var/spool (Verzeichnis für Warteschlangen; für Email, etc.)
  - Verzeichnis /var/log (Verzeichnis für log-Dateien)
  - Verzeichnis /root (Daten von Nutzer root)
  - Verzeichnis /home (Home-Verzeichnisse weiterer Nutzeraccounts)

**Anmerkung:** Die zwischengespeicherten Befunddateien sind NICHT Bestandteil des Backup!

## 13. Anhang

- IT-Konzept des Kommunikationsdienstleisters HL komm (HL komm\_IT-Konzept AlertsNet\_18.03.2013.pdf)