

# Technisches IT-Konzept

## Anhang zum Projektprotokoll Vers. 5



### Projektleiter:

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



Bundesministerium  
für Gesundheit

Gefördert vom Bundesministerium für Gesundheit  
Förderkennzeichen: IIA5-2512FSB114



**Version 4.0**

## 1. Inhaltsverzeichnis

1.	Inhaltsverzeichnis .....	2
2.	Abbildungsverzeichnis .....	2
3.	Glossar .....	3
4.	Systemkomponenten.....	3
5.	Technische Systeme.....	4
5.1.	Datenübertragung Labor zu MDDS (VPN) .....	4
5.2.	Zentrale Datenverarbeitende Systeme.....	4
6.	Rollen und Authentifizierung .....	6
6.1.	Authentifizierung .....	7
6.2.	Administrator Labore (Extern).....	7
6.3.	Kommunikations-Dienstleister (Extern) .....	7
6.4.	Administratoren/IT-Verantwortliche (Intern) .....	8
6.5.	Stammdatenpflege/AlertsNet-Arbeitsgruppe (Intern).....	8
6.6.	Nutzerpflege/AlertsNet-Arbeitsgruppe (Intern).....	8
6.7.	Dokumentare externe Versorgungseinrichtung/Klinische Einrichtungen (Extern) ...	8
7.	Administrative Prozesse .....	9
7.1.	Nutzerpflege .....	9
7.2.	Stammdatenpflege .....	9
7.3.	Systempflege .....	10
7.4.	Administration der unterliegenden Systeme .....	10
7.5.	Datenexport .....	10
7.6.	Laboranbindung .....	10
8.	Blutkulturbefund-Verarbeitung .....	11
8.1.	Befundimport .....	11
8.2.	Identifikation von Positivkulturen.....	15
9.	Benachrichtigung der Versorgungseinrichtung .....	15
10.	Kommunikation zwischen Microbiological Data Document System (MDDS) & Clinical Data Document System (CDDS).....	16
10.1.	eCRF-Eingabe .....	16
11.	Technische Dokumentation .....	18
11.1.	Mengengerüst .....	18
11.2.	Datenauswertung.....	18
11.3.	Datenhaltung .....	18
11.4.	Daten im Blutkultur-System:.....	19
11.5.	Daten im CDDS: .....	19
12.	Anhang.....	31

## 2. Abbildungsverzeichnis

<b>Abbildung 1:</b> Import-Prozess für BK-Befunddaten.....	14
<b>Abbildung 2:</b> Prozess der Dokumentation patientenbezogener klinischer Daten zu relevant- positiv getesteten BK-Befunden.....	17

### 3. Glossar

<b>Begriff</b>	<b>Beschreibung</b>
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. Technische Systeme

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

- **VPN-Gateway (Laborseitig)**

- Funktion: Stellt verschlüsselten Kommunikationskanal zu Bereitstellungsverzeichnis für BK-Nachrichten-Dateien beim Labordienstleister bereit
- Standort: beim Labordienstleister
- System VPN: VPN-Gateway (Box-Hardware), bereitgestellt durch Kommunikationsdienstleister
- Zugriffsberechtigung: Rolle Kommunikationsdienstleister (VPN-KommDL)
- Monitoring: VPN-KommDL  
Alternative: Ist der Datenabruf durch das MDDS nicht möglich erfolgt eine Meldung an VPN-KommDL
- Verschlüsselung des Kommunikationskanals gemäß geltender Standards

- **Quellenanbindung MDDS-Server**

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

### 5.2. Zentrale Datenverarbeitende Systeme

- **MDDS-Server**

- Funktion: Verarbeitung der Blutkulturbefund-Dateien  
Zentrale Datenhaltung  
Bewertung der Blutkulturbefunde  
Pseudonymisierung  
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)
- 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 Pseudonym-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

## 6. Rollen und Authentifizierung

Folgende Rollen sind in der informationstechnologischen Lösung von AlertsNet zwingend erforderlich, um einen reibungslosen Betrieb zu gewährleisten. 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.

## **6.1. 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 gewechselt werden, z. B. alle 90 Tage. Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht.
- Alte Passwörter sollten 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)).

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

Die Administratoren in den externen Laboren sind Ansprechpartner hinsichtlich der Bereitstellung der Befund-Nachrichten sowie der Struktur der Nachrichten.

## **6.3. Kommunikations-Dienstleister (Extern)**

Der Netzwerkdienstleister, 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.

#### **6.4. 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, Mappingpflege-Keime, Mappingpflege-Antiinfektiva).

#### **6.5. 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 Administration der Mappings für Keime und Antiinfektiva.

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

Um im laufenden Betrieb die administrative Rolle 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 Benutzer anzulegen und bestimmte, vorher festgelegte Gruppen zu vergeben. Andere Funktionen bzw. Rechte sind nicht erforderlich.

#### **6.7. Dokumentare externe Versorgungseinrichtung/Klinische 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. Administrative Prozesse

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

### 7.1. 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 Rechtematrix versehen. Somit ist es möglich, feingranuliert Anwendungsrechte zu vergeben. Die Zuordnung der Gruppen kann pro Benutzer eingeschränkt werden. Bestimmte Administrator-Rollen können nur bestimmte Gruppen vergeben. Die Nutzerpflege erfolgt ausschließlich im MDDS. Dieses transferiert die eCRF-Benutzer (klinische Dokumentare) auf das CDDS per Webservice.

### 7.2. 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 der einzelnen Einrichtungen aufgenommen und der jeweiligen Einrichtung zugeordnet. Beim Import der Blutkultur wird diese dann der entsprechenden Station (falls möglich) zugeordnet.

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.

Stations- und Einrichtungstypen werden ebenfalls gepflegt. Sie dienen der fachspezifischen Gruppierung der einzelnen Häuser und vor allem der Stationen. Auch hier ist die qualitative Verbesserung der Auswertungen zielgebend.

### **7.3. Systempflege**

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

### **7.4. Administration der unterliegenden Systeme**

Das Betriebssystem, voraussichtlich CentOS 6.x, muss fortlaufend überwacht und aktualisiert werden, die Logfiles unter /var/log sind regelmäßig zu prüfen. Auch der installierte Applicationserver (Tomcat oder Glassfish 3) und der Webserver müssen regelmäßigen Updates unterzogen werden. Die Aktualität der installierten Software-Pakete wird täglich per Nagios gegen ein zentrales Paket-Repository überprüft.

### **7.5. Datenexport**

Für Auswertungen werden die Daten im CSV Format exportiert. Der Datenexport erfolgt unter Verwendung einer SQL-Konsole direkt auf der Datenbank. Nur pseudonymisierte Daten werden exportiert. Der Datenbankzugriff erfolgt mit einem lesenden Benutzer unter eingeschränkten Rechten (nur exportrelevante Daten sind sichtbar). Den Export führen nur Systemadministratoren durch.

### **7.6. Laboranbindung**

Jeder neue Teilnehmer muss an die zentrale AlertsNet-Datenbank 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: Erhält er zum erwarteten Zeitpunkt keine Nachrichten von einem Labor, werden die Systemadministratoren des MDDS-Servers informiert.

## 8. Blutkulturbefund-Verarbeitung

### 8.1. Befundimport

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 oben). Da eine Patientenzuordnung erforderlich ist, sind innerhalb des Imports der HL7-Nachrichten auch die Stammdaten zu extrahieren. Diese umfassen Name, Vorname, Geburtsdatum, Geschlecht (Zuordnung zur Versorgungseinrichtung wird bereits durchgeführt). Weitere Daten werden nicht erfasst. Die Stammdaten werden pseudonymisiert (Patientenpseudonym). Zur Patientenpseudonymisierung werden Name, Vorname, Geburtsdatum, Geschlecht herangezogen. Bei Namen und Vornamen werden Sonderzeichen (ß,ä,ö,ü,é,ú,ó,á) in ASCII 128 umgesetzt. Anschließend werden die einzelnen Strings getrennt durch ein Pipe (|) Zeichen miteinander verkettet. Der hieraus entstehenden String wird dann per SHA-512 HASH-Algorithmus im java.security-Package verschlüsselt und gespeichert. Anhand des Patientenpseudonyms kann eine Nachverfolgung des Patienten realisiert werden, auch wenn dieser eine andere Einrichtung besucht. 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.

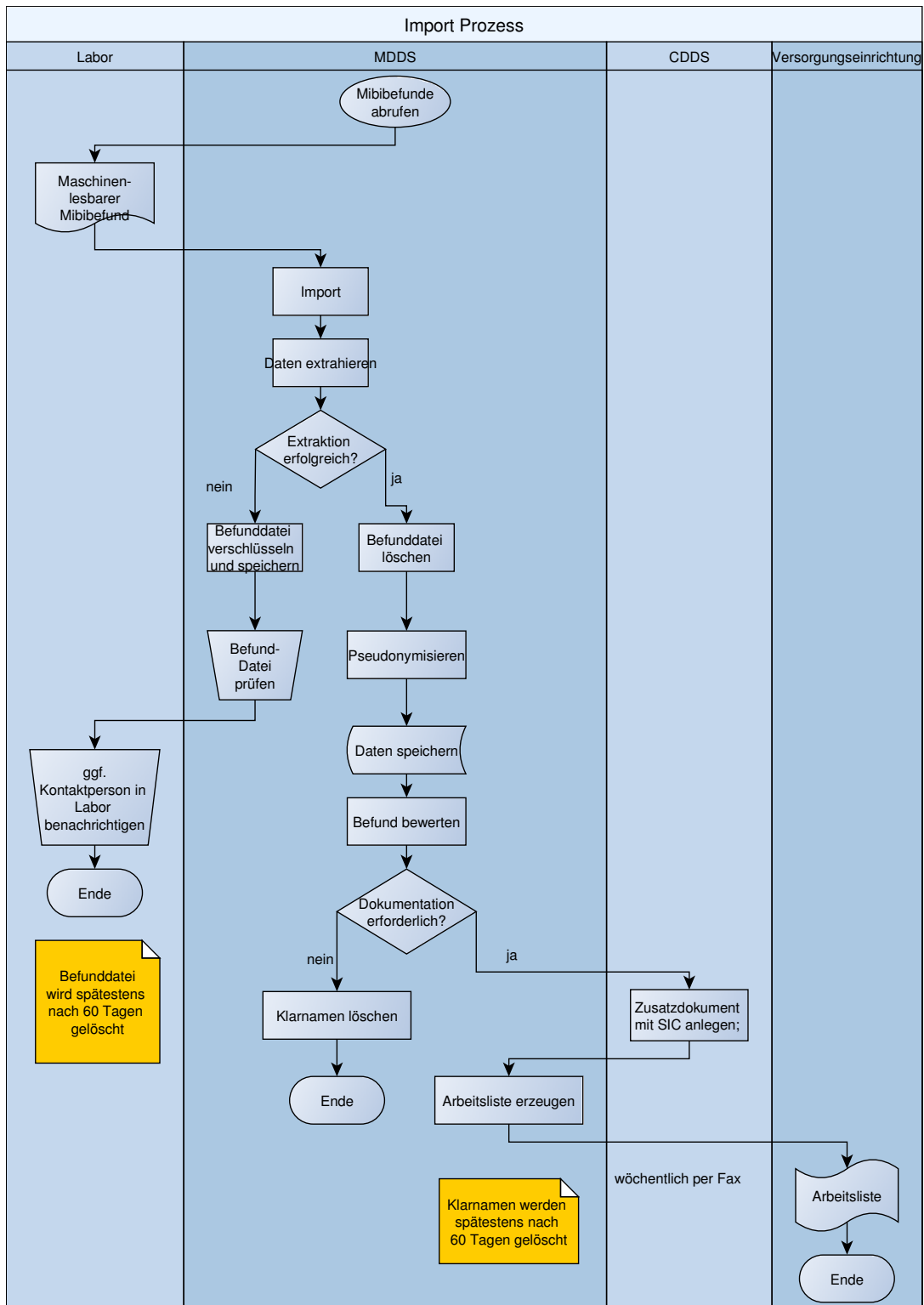
- Ein Löschprotokoll der Klarnamen kann vom Datenschützer der betroffenen klinischen Einrichtung angefordert werden. Der Bericht wird auf der Datenbankebene erzeugt und ist durch die Administratoren abrufbar.

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 des Primary Keys des einzelnen Befundes 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 zusammen.



**Abbildung 1: Import-Prozess für BK-Befunddaten.**

## 8.2. 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 Patient (Pseudonym) 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.
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 Antiinfektivgabe gilt ein Keim nach 12 Tagen als eliminiert.)

## 9. Benachrichtigung der Versorgungseinrichtung

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

Die Kontaktdaten und die Faxnummer werden in der Einrichtungskonfiguration des BK Systems per Eingabemaske gepflegt. Die Faxnummern werden monatlich validiert.

Bei Versenden der Faxnachricht wird nicht auf eine Versand-Bestätigung gewartet. Vielmehr werden für nicht erfolgte Dokumentationen die Daten erneut 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.

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.

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

Die Kommunikation zwischen dem MDDS und dem CDDS erfolgt unidirektional. 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.

### **10.1. eCRF-Eingabe**

In den Versorgungseinrichtungen (Projekteinrichtungen) erfolgt die ergänzende Dokumentation von Positivbefunden mittels eines Screening-Fragebogens. Der Fragebogen wird dabei im eigenentwickelten CDDS abgebildet. Die SICs werden vom MDDS-Server unidirektional im CDDS per Webservice angelegt.

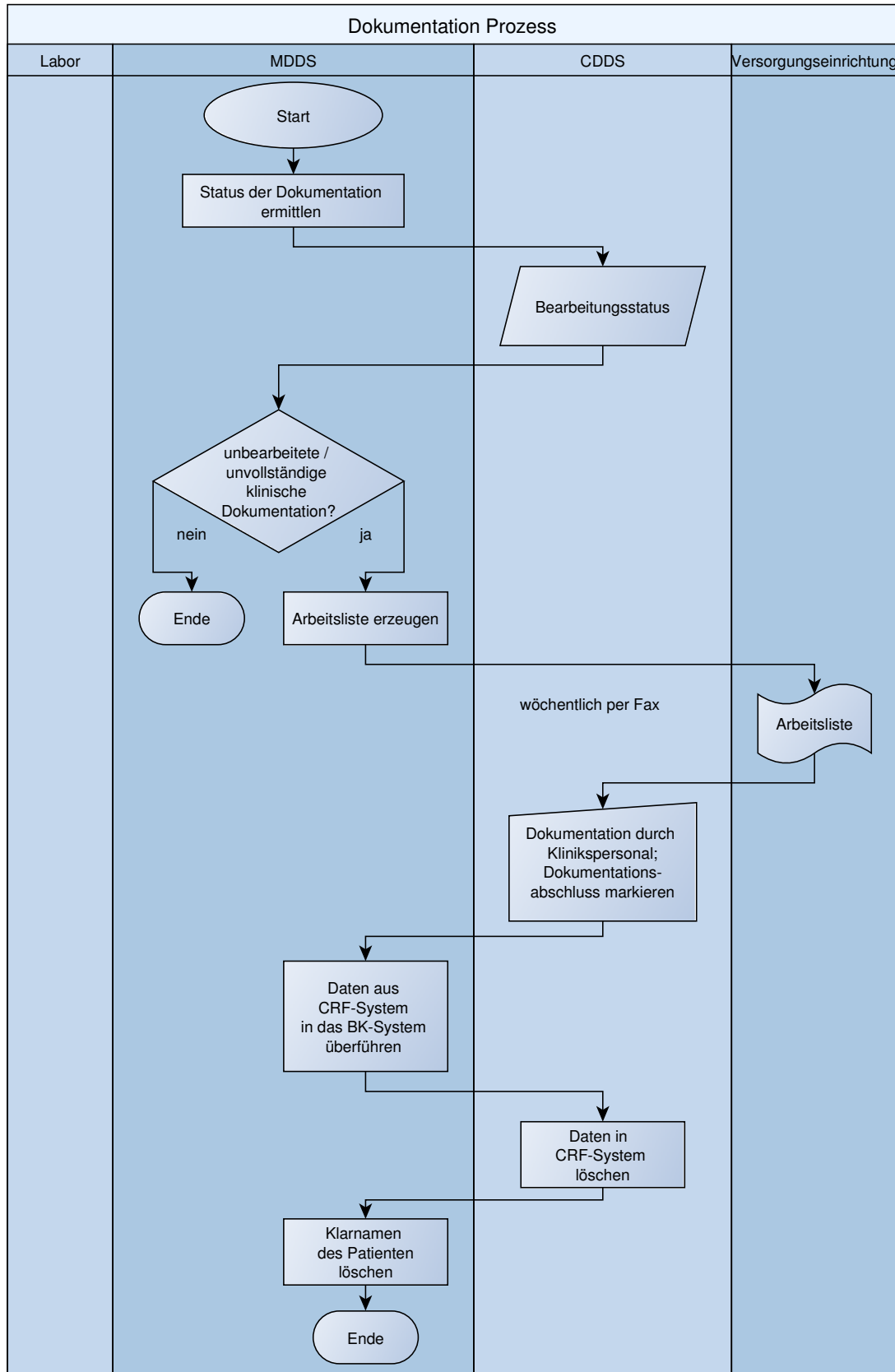
Um den Versorgungseinrichtungen die Möglichkeit der Zuordnung von Fällen zu SICs zu ermöglichen, generiert der MDDS-Server eine Faxnachricht an die entsprechende Versorgungseinrichtung. Die Nachricht enthält die Klarnamen-SIC Zuordnungen.

Die validen und nicht öffentlich zugänglichen Faxgeräte/Faxnummern sind ebenfalls im MDDS-Server pflegbar. Die Faxnummer ist ein Item in der Konfiguration der Versorgungseinrichtung.

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 des eCRF den angelegten Screening-Fragebogen 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.

## 11. Technische Dokumentation

### 11.1. Mengengerüst

Bettentage / 1.000 Patiente(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

### 11.2. 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.

### 11.3. 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.

**11.4. Daten im Blutkultur-System:**

- Administrativen Daten, Patienten, Blutkulturbefunde, Kontakte zu den Häusern, Stationen, Benutzer und Rechtemanagement, Mappings von Antiinfektiva und Keimen, Medikamente.
- 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.
- Klarnamen werden immer TripleDeS verschlüsselt gespeichert.
- Patienten werden per SHA512-Hash über Vorname, Nachname, Geburtsdatum und Geschlecht pseudonymisiert, Klarnamen werden gelöscht.
- Patienten ohne Positivbefunde werden sofort pseudonymisiert.

**11.5. Daten im CDDS:**

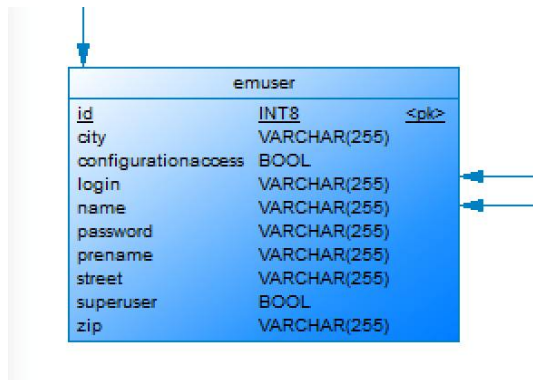
- Benutzer und Rechtemanagement, Blutkulturbefunde (ausschließlich die SIC), Patienten (ausschließlich Geburtsjahr und Geschlecht), Einrichtungen und Stationen, Medikamente.
- eCRF in vollständiger Ausprägung bis zur Abholung durch das Blutkultur-System.

Folgende Daten werden in der Datenbank gehalten:

**Benutzer**

<b>Bezeichnung</b>	<b>Datentyp</b>	<b>Bemerkung</b>
Name	Varchar	
Vorname	Varchar	
Login	Varchar	
Passwort	Varchar	
Beschreibung	Varchar	null
Konfigurations-Zugriff	Boolean	Pflege von Mappings, Einrichtungen, Nutzer
Superuser	Boolean	Systempflege
Zugehörigkeit zu Einrichtung	Referenz	

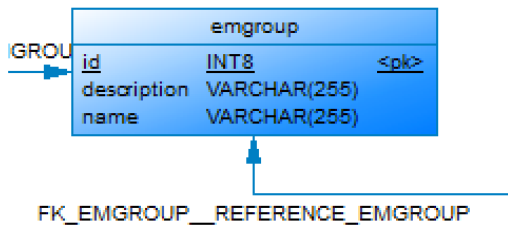
Tabelle im Datenmodell



**Gruppe**

Name	Varchar	
Beschreibung	Varchar	null

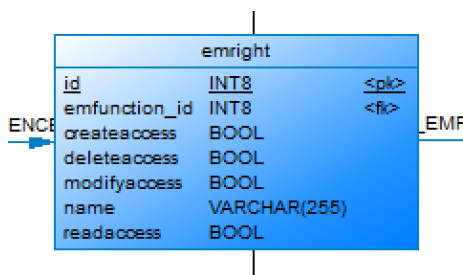
Tabelle im Datenmodell



**Recht**

Erstellen	Boolean	
Löschen	Boolean	
Modifizieren	Boolean	
Lesen	Boolean	

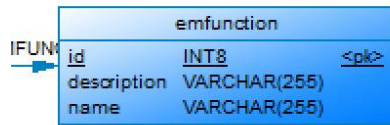
Tabelle im Datenmodell



**Funktion**

Name	Varchar	
Beschreibung	Varchar	null

Tabelle im Datenmodell

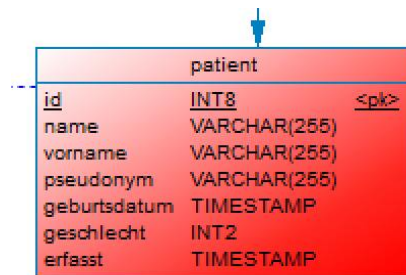


**Patient**

<b>Name</b>	<b>Varchar</b>	
<b>Vorname</b>	<b>Varchar</b>	
Pseudonym	Varchar	TBD
<b>Geburtsdatum</b>	<b>Date</b>	
<b>Geschlecht</b>	<b>int</b>	
erfasst	Date	TBD

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

Tabelle im Datenmodell



**Befund**

Patient	Referenz	
Labor	Referenz	
Einrichtung	Referenz	
Art der Blutkultur	Referenz	(anaerob/anaerob/beides) erforderlich?
Station	Referenz	
<b>Fallnummer</b>	varchar	
SIC	varchar	Identifikator
Probeeingang	Date	
Anforderung	Date	
Anzahl der Keime	int	
negativ	boolean	
Abnahmezeitpunkt	Date	
Eingangszeitpunkt	Date	
Berichtszeitpunkt	Date	
status	int	dokumentiert, versendet etc.
Crf_komplett	boolean	eCRF ausgefüllt

## Tabelle im Datenmodell

blut_befund		
id	INT8	<pk>
patient_id	INT8	<fk1>
labor_id	INT8	<fk2>
einrichtung_id	INT8	<fk3>
art_positiv_kultur_id	INT8	<fk4>
station_id	INT8	<fk5>
fallnummer	VARCHAR(255)	
sic	varchar(255)	
probeeingang	TIMESTAMP	
anforderung	TIMESTAMP	
anzahl_keime	INT2	
negativ	BOOL	
auftragsnummer	varchar(255)	
abnahmezeitpunkt	TIMESTAMP	
eingangszeitpunkt	TIMESTAMP	
berichtszeitpunkt	TIMESTAMP	
status	INT2	
orf_komplett	BOOL	

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: Zeitpunkt, wann Blutkultur positiv wurde
- Berichtszeitpunkt (= Erstellungszeitpunkt (Datum und Zeit ) des HL7-„Final Report“-Files)
- Patientenvorname, -nachname, Geburtsdatum und Geschlecht  
→ als Grundlage für einen pseudonymisierten HASH-String
- einsendende Einrichtung inkl. Abbildung der Organisationsstruktur
- Anzahl der nachgewiesenen Keime
- Art der positiven Kultur
- 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.

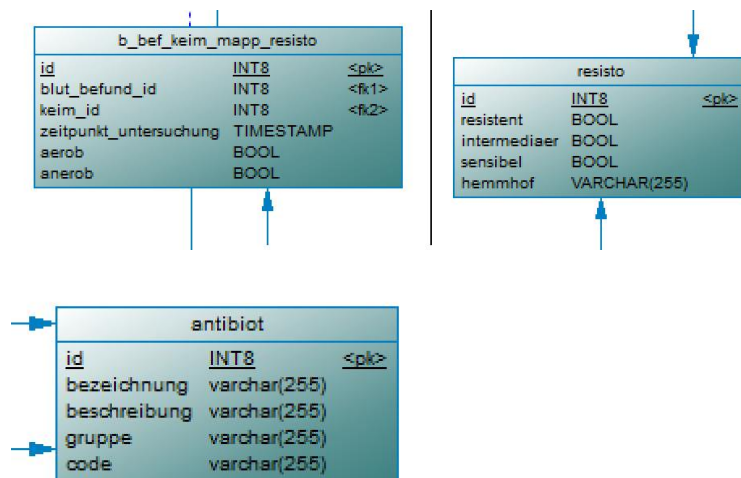
**Keim**

Bezeichnung	Datentyp	
Blutkulturbefund	Referenz	
Keim	Referenz	
Zeitpunkt der Untersuchung		
aerob	boolean	
anaerob	boolean	

**Resistogramm**

Bezeichnung	Datentyp	
Blutkulturbefund	Referenz	
Keim	Referenz	
Interpretierte Keimempfindlichkeit (S/I/R)	boolean	
Hemmhof	varchar	
Antiinfektiva	Referenz	

Tabellen im Datenmodell



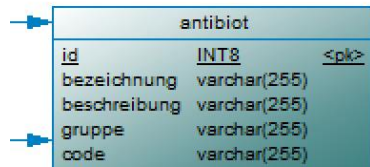
Resistogramm je Keim mit folgenden Subitemen:

- 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

**Antibiogramm (Einrichtungsunabhängig)**

Bezeichnung	Varchar	
Code	Varchar	
Gruppe	Varchar	
Beschreibung	Varchar	

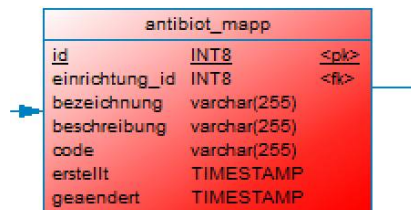
Tabelle im Datenmodell



**Antibiogramm Mapping (Einrichtungsabhängig)**

Einrichtung	Referenz	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
erstellt	Date	
geändert	Date	

Tabelle im Datenmodell



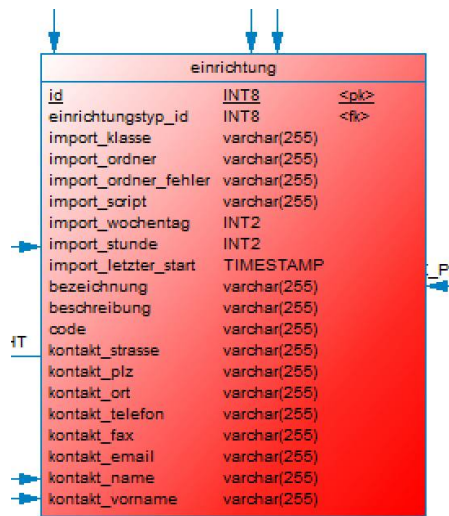
**Einrichtung**

Name	Varchar	
Einrichtungstyp	Referenz	
Import Klasse	Varchar	
Import Ordner	Varchar	
Import Ordner Fehler	Varchar	
Import Script	Varchar	
Import Wochentag	int	Sonntag 1
Import Stunde	int	
Import letzter Start	Date	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
Kontakt Name	Varchar	
Kontakt Vorname	Varchar	
Kontakt Strasse	Varchar	
Kontakt Ort	Varchar	



Kontakt Telefon	Varchar	
Kontakt Fax	Varchar	

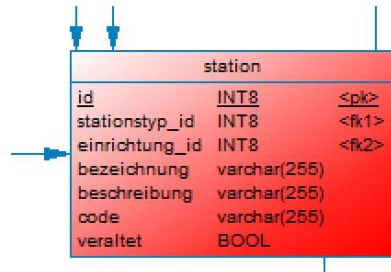
Tabelle im Datenmodell



**Station**

Name	Varchar	
Einrichtung	Referenz	
Stationstyp	Referenz	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
veraltet	Boolean	

Tabelle im Datenmodell



**Einrichtungstyp**

Name	Varchar	
Bezeichnung	Varchar	
Beschreibung	Varchar	

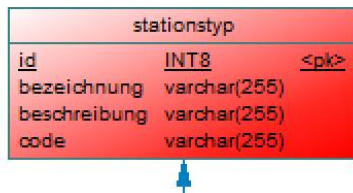
Tabelle im Datenmodell



### Stationstyp

Name	Varchar	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	varchar	

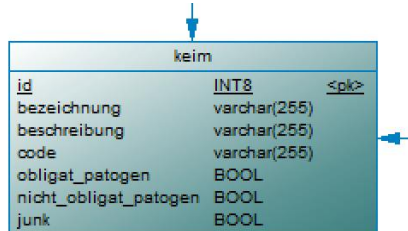
Tabelle im Datenmodell



### Keim (einrichtungsunabhängig)

Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
Obligat patogen	Boolean	
Nicht obligat patogen	Boolean	
Junk	Boolean	

Tabelle im Datenmodell



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

### Keim Mapping (einrichtungsabhängig)

Einrichtung	Referenz	
Keim	Referenz	
Bezeichnung	Varchar	
Beschreibung	Varchar	
Code	Varchar	
erstellt	Date	
geändert	Date	

## Tabelle aus Datenmodell

keim_mapp		
id	INT8	<pk>
einrichtung_id	INT8	<fk1>
keim_id	INT8	<fk2>
bezeichnung	varchar(255)	
beschreibung	varchar(255)	
code	varchar(255)	
erstellt	TIMESTAMP	
geändert	TIMESTAMP	

## eCRF (gemäß eCRF-Vorschlag)

Blutkulturbefund	Referenz auf Blutkulturbefund	
Station	Referenz auf Station	
Einrichtung	Referenz auf Einrichtung	
Benutzer	Referenz auf Benutzer	
Entlassung	Referenz Art der Entlassung	
Geburtsjahr	Int	
Geschlecht	Int	0 männlich 1 weiblich -1 unbekannt
Aufnahme Krankenhaus	Date	
Aufenthalt	Int	Aufenthalt in einer stationären Einrichtung
Datum Abnahme Blutkultur	Date	
Operation in den letzten 30 Tagen	Int	
Operationen	Referenz	OPS, Notfall
Zentraler Venenkatheter	Int	
Periphere Venenkanüle	Int	
Maschinelle Beatmung	Int	
Harnblasenkatheter	Int	
Ambulant erworben	Int	Infektionsursprung
Nosokomial	Int	
Allgemeinstation	Int	
ITS	Int	
Externe Einrichtung	Int	
unbekannt	Int	
Primäre Bakteriämie	Int	Infektionslokalisierung
ZNS	Int	Sekundäre Bakteriämie
Kardiovaskulär	Int	
Thorakal	Int	
Pneumonie	Int	
Sonstige Infektion	Int	
Intraabdominal	Int	
Gastrointestinal	Int	
Urogenital	Int	
Gefäßkatheterinfektion	Int	

Chirurgische Wundinfektion	Int	
Infektion der Knochen	Int	
Andere	Int	
unbekannt	Int	
Sepsis	Int	Maximaler Schweregrad der Infektion
Schwere Sepsis	Int	
Septischer Schock	Int	
KH Hauptdiagnose	Varchar	Entlassungsdiagnosen
Diabetes melitus		Nebendiagnosen nach ICD
Kardiovaskuläre Erkrankung	Int	
Cerebrovaskuläre Erkrankung	Int	
Renale Dysfunktion	Int	
COPD	Int	
Leberzirrhose	Int	
Tumorerkrankungen	Int	
Immunsuppression	Int	
Antimikrobielle Therapie	Int	Antimikrobielle Therapie
Antiinfektivum	Referent 1:N	
Therapie nach BK Abnahme	Int	
Antiinfektivum	Referenz 1:N	
Patient lag auf ITS	Int	Nacherhebung
Liegedauer	Referent 1:N	
Lebend Entlassen	Int	
Datum Entlassung/tot	Date	
Entlassung wohin	Referenz	
Welche Einrichtung	Varchar	

Tabelle im Datenmodell

orf		
id	INT8	<pk>
blut_befund_id	INT8	<fk1>
station_id	INT8	<fk2>
einrichtung_id	INT8	<fk3>
emuser_id	INT8	<fk4>
orf_entlassung_id	INT8	<fk5>
dd_geburtsjahr	INT2	
dd_geschlecht	INT2	
dd_datum_aufnahme_krankenhaus	DATE	
dd_aufenthalt	INT2	
sta_datum_abnahme_blutkultur	DATE	
rfns_op_30_tage	INT2	
rfns_zentraler_venenkatheter	VARCHAR(255)	
rfns_periphere_venekanuele	INT2	
rfns_maschinelle_beatmung	INT2	
rfns_harnblasenkatheter	INT2	
wuiu_ambulant_erworben	INT2	
wuiu_nosokomial	INT2	
wuiu_allgemeinstation	INT2	
wuiu_its	INT2	
wuiu_externe_einrichtung	INT2	
itbka_primaere_bakteriaemie	INT2	
itbka_sb_zns	INT2	
itbka_sb_kardiovaskulaer	INT2	
itbka_sb_thorakal	INT2	
itbka_sb_pneumonie	INT2	
itbka_sb_sonstige	INT2	
itbka_sb_intraabdominal	INT2	
itbka_sb_gastrointestinal	INT2	
itbka_sb_urogenital	INT2	
itbka_sb_gefaesskathinfektion	INT2	
itbka_sb_chrg_wundinfektion	INT2	
itbka_sb_knochen_weichteile	INT2	
itbka_sb_andere	INT2	
itbka_sb_unbekannt	INT2	
msi_sepsis_ohne_dysfkt	INT2	
msi_schwere_sepsis_mit_dysfkt	INT2	
msi_septischer_schock	INT2	
ed_kh_hauptdiagnose	VARCHAR(255)	
ed_nd_diabetes	INT2	
ed_nd_kardiovaskulaer	INT2	
ed_nd_cerebrovaskulaer	INT2	
ed_renale_dysfunktion	INT2	
ed_copd	INT2	
ed_leberzirrhose	INT2	
ed_solide_haem_tumor	INT2	
ed_therap_immunsupp	INT2	
at_zeitpunkt_bk_abnahme	INT2	
at_nach_bk_abnahme	INT2	
ne_patient_its	INT2	
ne_patient_lebend_entlassen	INT2	
ne_datum_entl_oder_verstb	DATE	
ne_entl_einrichtung	VARCHAR(255)	
abgeschlossen	BOOL	
status	INT2	

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 werden und die alte Station auf veraltet gesetzt werden.

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

## 12. Anhang

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