Deutsches Qualitätsbündnis SEPSIS

DSG Deutsche Sepsis-Gesellschaft

Anleitung zu Datenlieferung und Datenempfang

Anleitung für die Datenlieferung und den Datenempfang im Deutschen Qualitätsbündnis Sepsis

Inhalt

1 Datenlieferung 4

1.1 Einführung 4

1.2 Schritt 1: Formatierung der Daten im Format nach §21 KHEntgG 5

1.2.1 Datensatz 5

1.2.2 Datenschutz 6

1.3 Schritt 2: Technische Informationen zu Datenreduzierung, Pseudonymisierung und Verschlüsselung der Daten 6

1.3.1 3M-CryptoWizard DQS-Version 6

1.3.2 Download und öffnen des CryptoWizard 7

1.3.3 Erläuterungen zur Funktionalität des CryptoWizard bzgl. der Datenlieferung 9

1.4 Schritt 3: Ihre Daten pseudonymisieren, reduzieren und verschlüsseln 11

1.4.1 Persönliches PGP-Schlüsselpaar erzeugen 11

1.4.2 Ihre Daten verschlüsseln 12

1.5 Schritt 4: Daten an cuviba liefern 16

1.5.1 Einführung zum cuviba Portal 16

1.5.2 Daten Hochladen 17

2 Ergebnisse von cuviba erhalten 17

2.1 Kodierübersicht herunterladen 17

2.2 Einzelfallliste herunterladen und entschlüsseln 18

2.3 Einzelfallliste depseudonymisieren 20

3 Anhang 27

3.1 Anhang 1 27

Kontakte:

Bei Fragen zu DQS-Qualitätsberichten oder Ihrer Einzelfallliste wenden Sie sich bitte an Anna-Meagan Fairley (anna-meagan.fairley@med.uni-jena.de, Tel: +49 3641 9 323183)

Bei Fragen zu Datenlieferungsprozessen und dem cuviba Datenportal wenden Sie sich bitte an cuviba (info@cuviba.com, Tel: +49 176 23 93 36 52)

1 Datenlieferung

In diesem Kapitel führen wir Sie Schritt für Schritt durch die DQS-Datenlieferung an unseren Dienstleister cuviba. Was Sie dafür benötigen, sind die §21-Daten Ihres Hauses, sowie den DQS-CryptoWizard, den Sie unter folgendem Link kostenlos herunterladen können:

https://3mhisdataservices.com/download/dqs/CryptoWizardDQS.zip

Die Daten in dieser Anleitung sind künstlich erstellte Beispieldaten ohne Bezug auf reale Patient:innen. Sollten Fragen auftreten, zögern Sie nicht, sich damit an uns zu wenden, wir gehen die Prozesse auch gerne mit Ihnen durch.

1.1 Einführung

Zur Vorbereitung der Datenlieferung müssen folgende Schritte umgesetzt werden:

1. Export der Daten im Format nach §21-KHEntgG aus dem Krankenhausinformationssystem
2. Pseudonymisierung der Daten, d.h. Ersetzung der KH-internen Fallnummer durch ein Pseudonym und Speicherung einer Schlüsseltabelle
3. Verschlüsselung der Daten für cuviba mit PGP-Verfahren

Zur Umsetzung des Schrittes 1 verwenden Sie die Funktionalität Ihres Krankenhausinformationssystems. In den Abteilungen für Medizincontrolling der Krankenhäuser besteht hierzu in der Regel umfängliche Erfahrung. Zur Vereinfachung Ihrer internen Prozesse, sollte dieselbe Person, die die Datenlieferung umsetzt, auch den Datenempfang wahrnehmen, d.h. die Einzelfallliste downloaden, entschlüsseln, und depseudonymisieren. Weitere Details zur Formatierung der zu liefernden Daten finden Sie in „Schritt 1: Formatierung der Daten im Format nach §21 KHEntgG“.

Für die Schritte 2 und 3 wird der 3M-CryptoWizard in einer speziellen DQS-Version bereitgestellt. Dieser vollzieht beide Schritte gleichzeitig. Sofern für diese Verarbeitungsschritte bei Ihnen bereits Prozesse etabliert sind und andere Software zum Einsatz kommt, können Sie diese Prozesse wie gewohnt umsetzen. Anleitung und Support können das DQS-Koordinationsbüro und cuviba jedoch nur für die Umsetzung mittels des DQS-CryptoWizard gewährleisten.

1.2 Schritt 1: Formatierung der Daten im Format nach §21 KHEntgG

1.2.1 Datensatz

Zur Durchführung der Datenverarbeitung senden Sie uns Ihre Daten nach §21 KHEntgG (Inhalt und Aufbau in Anlehnung an offizielle Spezifikation (jedoch pseudonymisiert) in einer gültigen Fassung nach §21 KHEntgG).
Bitte beachten Sie, dass die Datensätze keine Anführungszeichen (“) enthalten dürfen. Dies passiert z.B. manchmal im Wohnort. Bitte entfernen Sie diese vor dem Versand. Sie können das z.B. über das Menü Bearbeiten -> Suchen und Ersetzen des Editors durchführen.

Benötigte Dateien:

- fall.csv
- fab.csv
- icd.csv
- ops.csv
- entgelte.csv

Bitte **bearbeiten Sie die Dateien nicht mit MS Excel**, um die Veränderung von Inhalten durch Autoformatierung zu vermeiden.

1.2.1.1 Standorte kennzeichnen

Bei Krankenhäusern mit gemeinsamem Institutskennzeichen (IK) und mehreren Standorten müssen diese im Feld „Entlassender-Standort“ gekennzeichnet werden. Alternativ kann auch standortgetrennt übermittelt werden, d.h. in separaten Datenlieferungen je Standort.

1.2.1.2 Fallzusammensetzung

Für die optimale Auswertung der Daten müssen folgende Voraussetzungen im Datensatz erfüllt sein.

- alle abgerechneten und nicht abgerechneten Fälle aller Abrechnungsarten (DRG Fälle, hausindividuell verhandelte Fälle, nach § 6 KHEntgG, Integrierte Versorgung),

- alle Versicherungsarten (GKV, Privat, GUV, Selbstzahler u.a.),
- alle vollstationären Fälle sind enthaten.
- Der Export ist abgegrenzt nach Entlassungsdatum. Überlieger des Vorjahres sind somit einzuschließen.
- Export nach Anwendung der Fallzusammenführung gemäß der Wiederaufnahmeregelung (siehe FPV).
- optional können Fälle aus psychiatrischen Abteilungen geliefert werden
- teilstationäre oder ausschließlich vorstationäre Fälle und Begleitpersonen können mitgeliefert werden, werden bei der Auswertung jedoch nicht berücksichtigt
- kumuliert: alle Fälle des aktuellen Auswertungsjahres in einem Datensatz
- verschlüsselt

1.2.1.3 Quartale

Die §21-Datenlieferungen erfolgen kumulativ, d.h. die schon vorher gelieferten Daten desselben Jahres werden nochmals mitgeliefert. Die Einordnung in Quartale erfolgt nach Entlassungsdatum. In der Jahresauswertung werden daher die zuvor gelieferten Daten des 1. Bis 3. Quartals überschrieben, so dass zwischenzeitlich erfolgte Änderungen automatisch berücksichtigt werden.

1.2.2 Datenschutz

Bitte achten Sie darauf, nur pseudonymisierte Datensätze zu senden und selbst Ihre Mapping-Tabelle aufzubewahren. Sie können die Daten mit einer krankenhauseigenen Software pseudonymisieren oder den DQS-Cryptowizard (https://3mhisdataservices.com/download/dqs/CryptoWizardDQS.zip) für diesen Prozess verwenden.

1.3 Schritt 2: Technische Informationen zu Datenreduzierung, Pseudonymisierung und Verschlüsselung der Daten

1.3.1 3M-CryptoWizard DQS-Version

Der 3M™ DQS-CryptoWizard (weiterhin nur CryptoWizard) ist eine Alternative zu anderen verfügbaren kommerziellen oder Open Source-Verschlüsselungstools mit dem Ziel, den Austausch von sensiblen Daten mit cuviba mit etablierten Verschlüsselungsverfahren abzusichern. Dabei soll er in der Inbetriebnahme und

im Gebrauch einfacher zu verwenden sein als die verfügbaren Alternativen. Der Standard-Crypto-Wizard ist auf die Verwendung innerhalb der Initiative Qualitätsmedizin (IQM) und den Datendienstleister solventum (ehemals 3M-Health-Inforation-Systems) ausgelegt. Für das DQS wurde eine spezialisierte Version des Cryptowizard erstellt, der eine einfache Datenlieferung an den DQS-Datendienstleister cuviba gewährleistet. **Bitte nutzen Sie stets die korrekt DQS-Version des CryptoWizard, sonst kann cuviba Ihre Daten nicht verarbeiten.**

Neben der Vorbereitung für den Datenversand bietet der DQS-CryptoWziard auch die Möglichkeit der Entschlüsselung der Einzelfallliste oder anderer sensibler Daten, die Ihnen durch cuviba zugesendet werden (Details im Abschnitt 2).

Systemanforderungen des 3M-CryptoWizard

- Betriebssystem: Windows 7, Windows 8 oder Windows 10 (Windows XP wird nicht unterstützt)
- Notwendige Nutzerrechte:
    - Administrator-Berechtigungen nicht erforderlich (keine Installation)
    - Vollzugriff auf Ordner für persönliche Dokumente („Eigene Dateien“, „Eigene Dokumente“, Bibliothek „Dokumente“ o.ä.)
    - Ausführbarkeit von Java-Anwendungen (das erforderliche Java Runtime Environment OpenJDK 17 JRE wird mitgeliefert)
    - Möglichkeit zum Entpacken von ZIP-Archiven

1.3.2 Download und öffnen des CryptoWizard

Laden Sie den CryptoWizard über folgenden Link herunter:

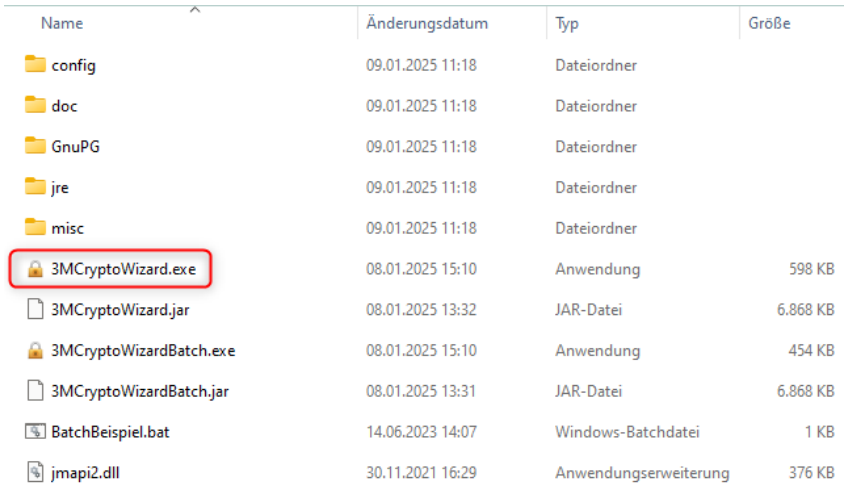
https://3mhisdataservices.com/download/dqs/CryptoWizardDQS.zip

Speichern Sie das ZIP-Archiv in einem Ordner auf den Vollzugriff besteht, wie z. B. Ihren persönlichen Dokumentenordner oder Desktop.

Eine Installation des CryptoWizard ist nicht erforderlich. Das heruntergeladene ZIP-Archiv (CryptoWizardDQS.zip) muss lediglich vor dem Starten vollständig entpackt werden. Alle zur Ausführung benötigten Ressourcen werden mitgeliefert.

Entpacken Sie das ZIP-Archiv mit Hilfe eines geeigneten Tools oder mit Windows-Bordmitteln vollständig in einen Unterordner, indem Sie mit der rechten Maustaste auf das ZIP-Archiv klicken und den Befehl „Alle extrahieren…“ ausführen.

Starten Sie die im Unterordner enthaltene Anwendungsdatei „3MCryptoWizard.exe“ per Doppelklick (Abbildung 1).



Name	Änderungsdatum	Typ	Größe
config	09.01.2025 11:18	Dateiordner	
doc	09.01.2025 11:18	Dateiordner	
GnuPG	09.01.2025 11:18	Dateiordner	
jre	09.01.2025 11:18	Dateiordner	
misc	09.01.2025 11:18	Dateiordner	
3MCryptoWizard.exe	08.01.2025 15:10	Anwendung	598 KB
3MCryptoWizard.jar	08.01.2025 13:32	JAR-Datei	6.868 KB
3MCryptoWizardBatch.exe	08.01.2025 15:10	Anwendung	454 KB
3MCryptoWizardBatch.jar	08.01.2025 13:31	JAR-Datei	6.868 KB
BatchBeispiel.bat	14.06.2023 14:07	Windows-Batchdatei	1 KB
jmapi2.dll	30.11.2021 16:29	Anwendungserweiterung	376 KB

Abbildung 1

Wenn Sie den CryptoWizard öffnen, werden Sie zuerst gebeten, die Nutzungsbedingungen zu akzeptieren (Abbildung 2). Stimmen Sie zu, öffnet sich das Hauptmenü des CryptoWizard. Um den CryptoWizard zu schließen, klicken Sie auf „Beenden“.

Abbildung 2

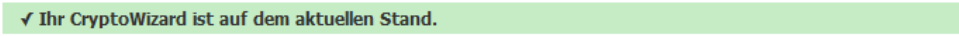
Hauptmenü

Im Hauptmenü können Sie alle Funktionalitäten des CryptoWizard anwählen (Abbildung 3). Welche Funktion für Sie gerade relevant ist, ergibt sich aus der Einteilung in die zwei Rubriken „Daten an den DQS IT-Dienstleister senden“ sowie „Ergebnisse vom DQS IT-Dienstleister erhalten“.

Abbildung 3

Sollte eine neuere Version des CryptoWizard zum Download bereitstehen, erhalten Sie oberhalb des Hauptmenüs einen entsprechenden Hinweis. In diesem Fall können Sie direkt auf den dort angezeigten Link klicken, um die neue Version herunterzuladen.

Ist jedoch die von Ihnen verwendete Version die neuste, wird auch das oberhalb des Hauptmenüs angezeigt:



1.3.3 Erläuterungen zur Funktionalität des CryptoWizard bzgl. der Datenlieferung

Datenpseudonymisierung

Bei der Aufbereitung der Daten nach § 21 KHEntgG führt der CryptoWizard ein automatisches Mapping der Fallnummern durch. Dabei wird die Original-Fallnummer gegen ein Pseudonym ausgetauscht. Gleichzeitig wird bei diesem

Vorgang eine Mappingdatei erzeugt, die im Krankenhaus verbleibt und später eine Rückübersetzung vom Pseudonym zur Original-Fallnummer ermöglicht.

Hinweis: Bitte laden Sie immer einen Original-§ 21-Datensatz in den CryptoWizard. Nutzen Sie bitte zuvor keine weitere Pseudonymisierungs-Funktion (z. B. über die KIS-Schnittstelle oder ein anderes Tool zur Pseudonymisierung). Andernfalls ist keine Rückübersetzung zur Original-Fallnummer gewährleistet.

Datenreduzierung

In diesem Arbeitsschritt entfernt der CryptoWizard alle Inhalte des § 21-Datensatzes, die nicht zur Ergebnisberechnung erforderlich sind. Das Tool berücksichtigt grundsätzlich nur die § 21-Dateien „FALL“, „FAB“, „ICD“, „OPS“ und „ENTGELTE“ in allen standardisierten Ausprägungen und aktuellen Versionen. Weitere Dateien bleiben unberücksichtigt und werden nicht mit verschlüsselt.

Innerhalb der Dateien werden die Inhalte bestimmter Datenfelder entweder ganz entfernt oder soweit reduziert bzw. verändert, dass kein Rückschluss auf den Original-Inhalt möglich ist. Anhang 1 gibt Ihnen eine Übersicht der Veränderungen.

Datenverschlüsselung

Der DQS-CryptoWizard hält sich an die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Es wird eine hybride Verschlüsselung nach dem OpenPGP-Standard unter Verwendung der Software „GNU Privacy Guard“ (GnuPG) genutzt:

1. Nachrichtenverschlüsselung mit symmetrischem Algorithmus AES-256
2. Session-Key-Verschlüsselung unter Verwendung asymmetrischer Algorithmen:
    a. Übertragung zu cuviba → asymmetrische Verschlüsselung mit 4096 Bit RSA-Schlüssel
    b. Übertragung zum Nutzer → asymmetrische Verschlüsselung mit 4096 Bit RSA-Schlüssel

1.4 Schritt 3: Ihre Daten pseudonymisieren, reduzieren und verschlüsseln

In diesem Abschnitt führen Wir Sie durch die Pseudonymisierung und Verschlüsselung Ihrer Daten für die Lieferung an cuviba. Bitte beachten Sie das alle hier verwendete Abbildungen Beispielhaft sind – Ihre eigenen Dateien und Ordner sind wahrscheinlich anders benannt.

1.4.1 Persönliches PGP-Schlüsselpaar erzeugen

Falls Sie zuvor noch keine Dateien mit dem CryptoWizard entschlüsselt haben müssen Sie zuerst ein *neues Schlüsselpaar* erstellen (Abbildung 4). Im Hauptmenü wählen Sie zunächst die Schaltfläche:

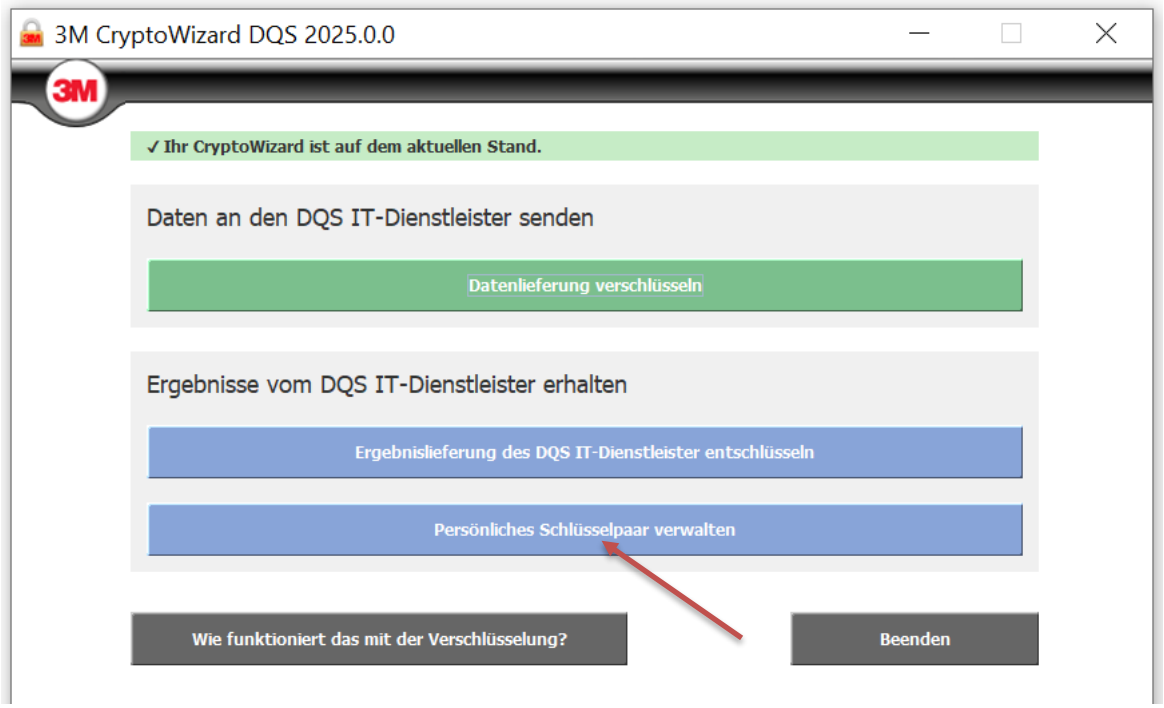


Abbildung 4

Nun folgen Sie den Instruktionen im neuen Fenster. Geben Sie Ihre Daten in die Oberfläche ein und wählen Sie dann die Schaltfläche „Schlüsselpaar erzeugen“ (Abbildung 5).

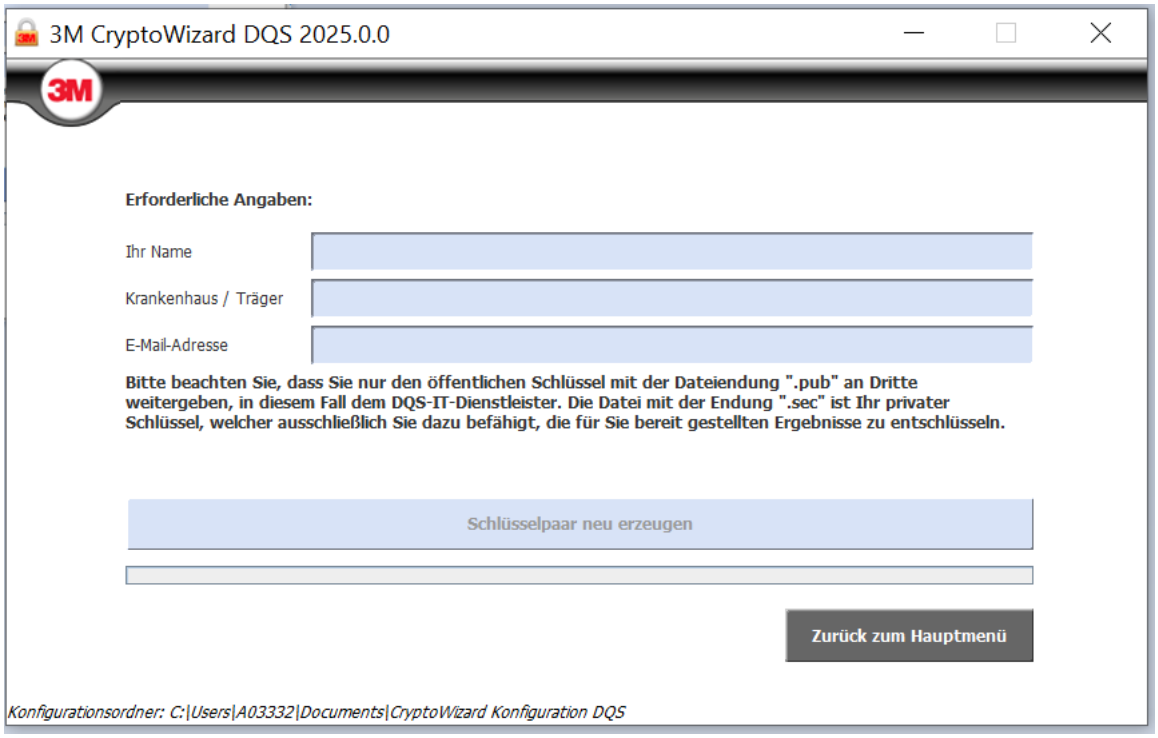


Abbildung 5

Der CryptoWizard erstellt Ihnen ihr Schlüsselpaar in der Regel in ihrem Dokumenteordner. Suchen Sie nach „CryptoWizard Konfiguration DQS“, dort finden Sie ihren Schlüssel. **Verschieben Sie diesen Ordner nicht**, da der CryptoWizard darauf zugreift um Ihre Verschlüsselung und Entschlüsselung zu machen und wenn der Ordner nicht gefunden wird kann der Prozess nicht ablaufen. Der öffentliche Schlüssel wird auch auf ihrem Desktop abgelegt.

WICHTIG: Geben Sie **ausschließlich ihren öffentlichen Schlüssel** an cuviba weiter (dieser hat das Format *Vorname_Nachname.pub*), niemals Ihren geheimen Schlüssel.

Wenn cuviba Ihren Schlüssel erhalten hat können Sie in Zukunft von cuviba verschlüsselte Dateien problemlos entschlüsseln. So zum Beispiel Ihre Einzelfallliste.

1.4.2 Ihre Daten verschlüsseln

Über den grünen Button „Datenlieferung verschlüsseln“ im Hauptmenü des CryptoWizard (Abbildung 3) erreichen Sie das Fenster in dem Sie Ihre Daten

pseudonymisieren und verschlüsseln können (Abbildung 6). Markieren Sie das Feld „§21 Daten (inkl. Pseudonymisierung)“.

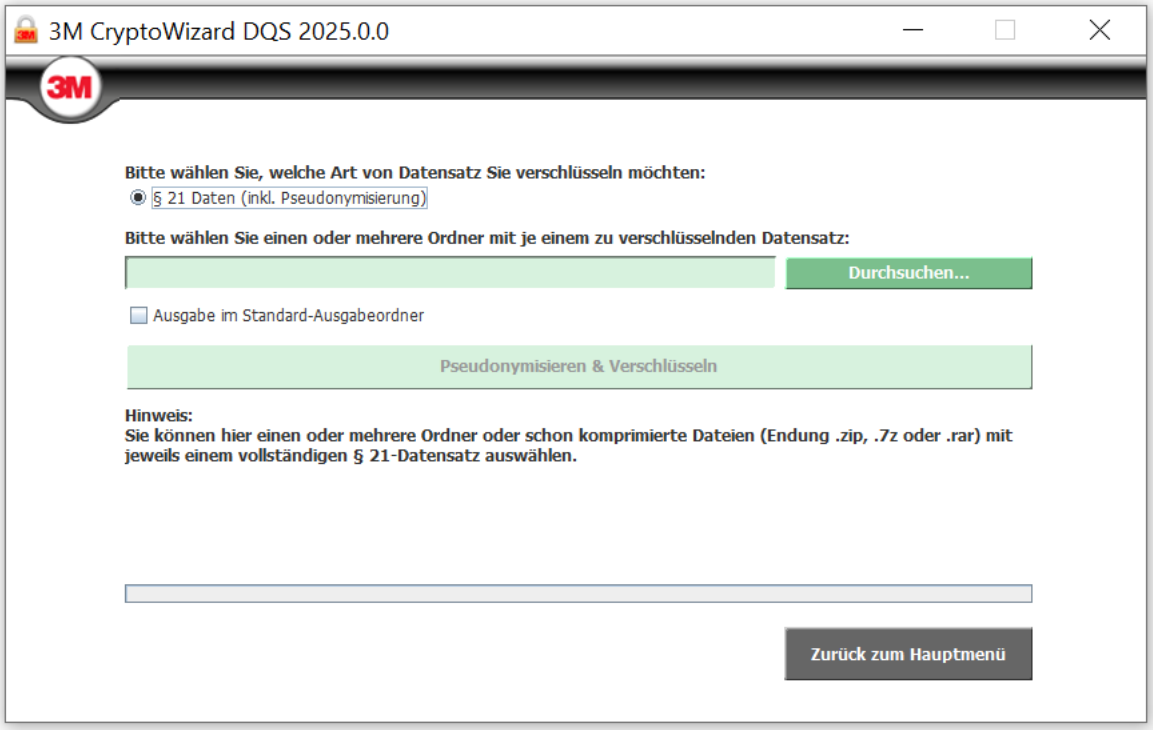
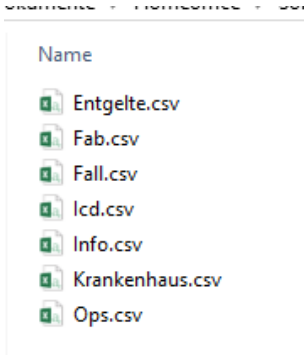


Abbildung 6

Klicken Sie zum Auswählen Ihrer Datensätze auf „Durchsuchen...“ und suchen Sie den Ordner, in dem Ihre exportierten §21 Daten liegen. Diese sehen in etwa wie folgt aus (enthalten sein müssen Fall, Icd, Ops, Fab, Entgelte).



Sie können den kompletten Ordner, in dem die Dateien liegen, auswählen.

Wenn Sie die Option „Ausgabe in Standard Ausgabeordner“ auswählen speichert der CryptoWizard die neuen Dateien in einem eigens dafür erstellten Order „CryptoWizard Ausgabe DQS“. Haben Sie das Feld nicht ausgewählt speichert der CryptoWizard die Dateien stattdessen am selben Ort, von wo Sie zuvor die Dateien hochgeladen haben. Klicken Sie nun auf „Pseudonymisieren & Verschlüssel“. Der Cryptowizard startet nun eine Prüfung, ob die angegebenen Daten im korrekten Format sind (Abbildung 7). Bestätigen Sie mit Fortfahren. Anschließend durchläuft der CryptoWizard die Pseudonymisierung und Verschlüsselung.

Abbildung 7

WICHTIG: Der Pfad unter dem die Dateien gespeichert werden, wird Ihnen angegeben (Abbildung 8). In diesem Ordner liegen die pseudonymisierten und verschlüsselten Daten – einschließlich der Mapping Datei, die Sie später wieder benötigen. Notieren Sie sich diesen Ordner, um spätere Unklarheit zu vermeiden.

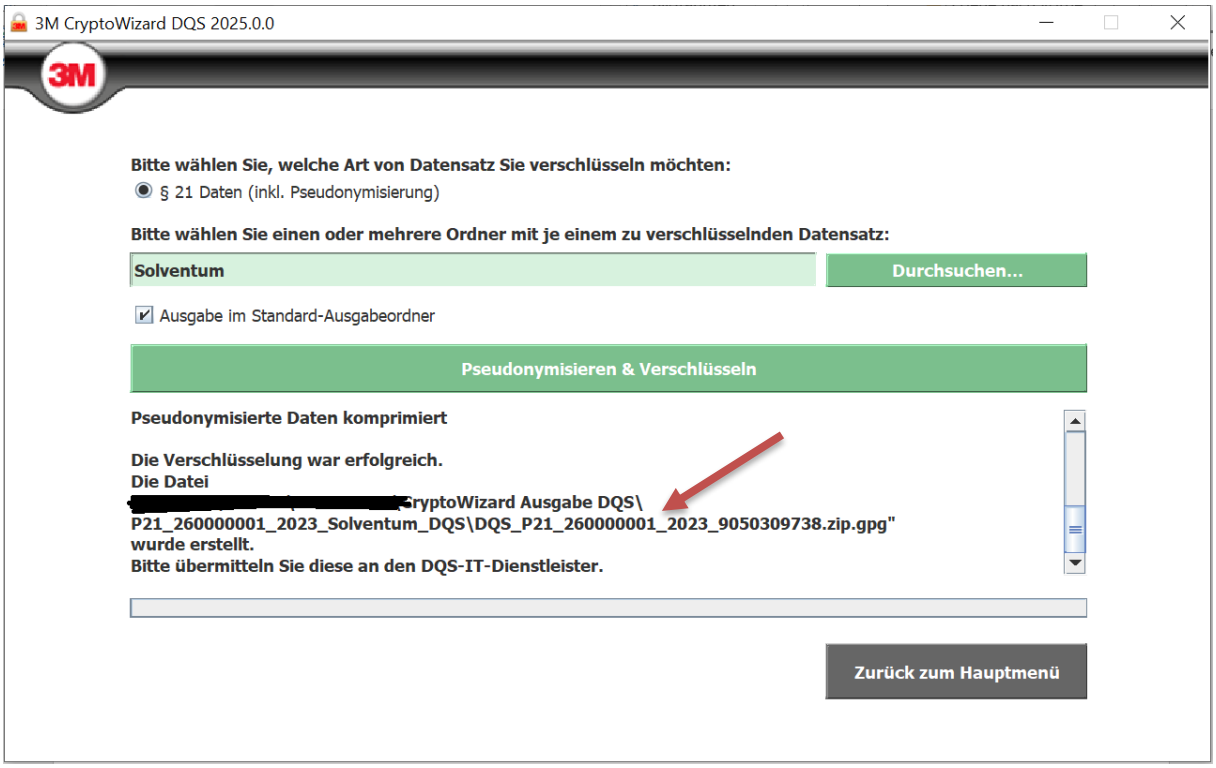


Abbildung 8

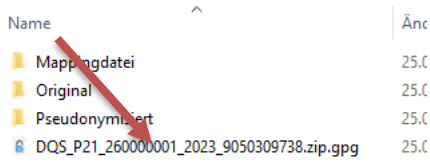


Abbildung 9

Finden Sie nun den angegebenen Ordner in Ihrem System. Darin finden Sie drei Ordner (Abbildung 9). Die Originaldaten befinden sich im Ordner „Original“, die Mappingdatei selbsterklärend im Ordner „Mappingdatei“, und die pseudonymisierten Daten im Ordner „Pseudonymisiert“. Zusätzlich enthält dieser Ordner die verschlüsselte Datei. Diese Datei können Sie genau so im Datenportal für cuviba hochladen. Sie erkennen diese Datei an der .gpg-Endung und dem kleinen Schloss-Icon. Die Mappingdatei brauchen Sie, um später Ihre Einzelfallliste zu de-pseudonymisieren.

WICHTIG: Die erstellte Mapping-Datei enthält ein Zufallspseudonym, d.h. die gleiche Fallnummer wird bei mehrmaligem Umsetzen der Pseudonymisierung (z.B. konsekutive Datenlieferungen oder erneuter Export gleicher Daten) NICHT in allen Versionen der Mapping-Datei das gleiche Pseudonym haben. Das bedeutet ihre **Mapping-Datei kann nur die Daten der letzten Lieferung depseudonymisieren**. Für

ältere Daten benötigen Sie demnach auch die älteren Mappings – daher ist es wichtig, alte Mapping Dateien zu sichern.

1.5 Schritt 4: Daten an cuviba liefern

1.5.1 Einführung zum cuviba Portal

Das cuviba Portal besteht inhaltlich aus zwei Teilen

1. dem “Datenportal” (zum Upload der §21-Daten und zum Download der Einzelfalllisten)
2. dem “Benchmarkserver” (zum Vergleich der adjustierten aggregierten Ergebnisse)

Datensender sehen nach dem Einloggen nur das Datenportal. Datenempfänger sehen beide Teile.

1.5.1.1 Erstes Einloggen, Schritt für Schritt

Wenn Sie von cuviba Zugangsdaten erhalten haben folgen Sie diesen Schritten. Falls Sie noch keine Zugangsdaten haben melden Sie sich unter info@cuviba.com mit ihrem Namen und dem Namen ihres Krankenhauses.

Folgen Sie dem Link zu http://dqs.cuviba.com/

Erlauben Sie Cookies

Klicken Sie auf Anmelden, geben Sie Ihre Nutzerdaten ein (diese erhalten Sie von cuviba) und bestätigen Sie diese.

Erlauben Sie nun dem Benchmarkserver Zugriff, inden Sie auf “Grant access” klicken.

Sie sind eingeloggt

Hinweis: Dieser Prozess mit Einloggen und Zugang erlauben erscheint aufwändig. Er ist aber nötig, weil der eigentliche Nutzer über das Datenportal verwaltet wird und der Benchmarkserver denselben Account nutzt.

1.5.2 Daten Hochladen

Bitte liefern Sie die Daten ausschließlich über das cuviba-Portal. Loggen Sie sich hierzu in Ihrem Cuviba Portal ein, wählen Sie den Reiter „Datenportal“ aus und gehen Sie hier in den Ordner des Hauses für das Sie Daten liefern (Abbildung 10). Klicken Sie dann auf „+New“ und „Upload files“. In dem folgenden Fenster wählen Sie die Datei aus, die sie hochladen möchten und bestätigen mit „Öffnen“, um Ihre Daten an cuviba zu liefern. Hier können Sie später auch Ihre Einzelfallliste finden und herunterladen.

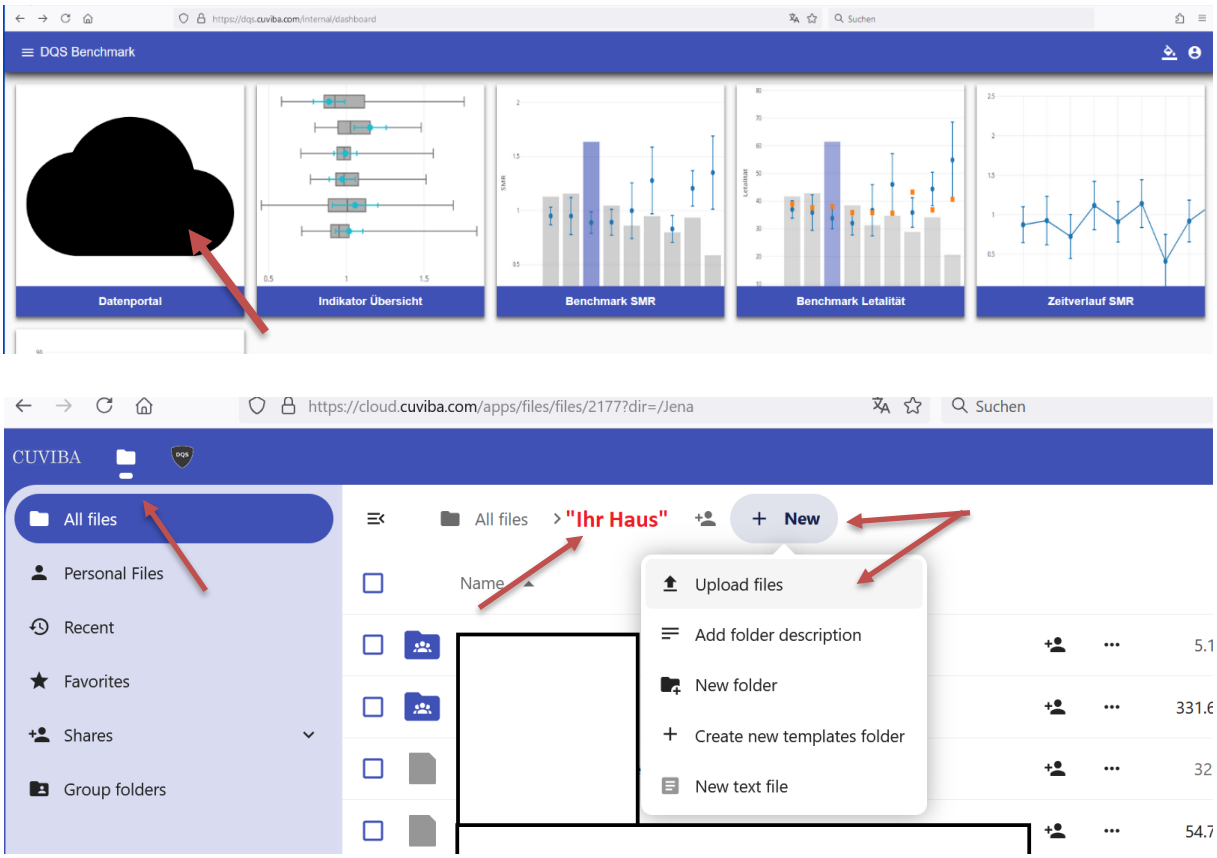


Abbildung 10

Sofern Sie Fragen rund um das Portal haben, oder Funktionsstörungen auftreten, wenden Sie sich bitte an cuviba (s. Kontaktangaben am Beginn des Dokuments).

2 Ergebnisse von cuviba erhalten

2.1 Kodierübersicht herunterladen

Ihre Kodierübersicht finden Sie in Ihrem Datenportal, für Gewöhnlich mit dem Namen „kodierübersicht_“und dem Namen Ihres Hases oder Ihrer Stadt. Diese Datei ist **unverschlüsselt**, da sie keine sensiblen Daten enthält, und kann einfach

heruntergeladen und geöffnet werden. Klicken Sie einfach auf die Datei in Ihrem Portal und ein Fenster öffnet sich mit der Aufforderungeinen Speicherplatz zu wählen.

2.2 Einzelfallliste herunterladen und entschlüsseln

Ihre Einzelfallliste finden Sie in Ihrem Datenportal bei cuviba. Dies sollte bei Ihnen in etwa so aussehen:

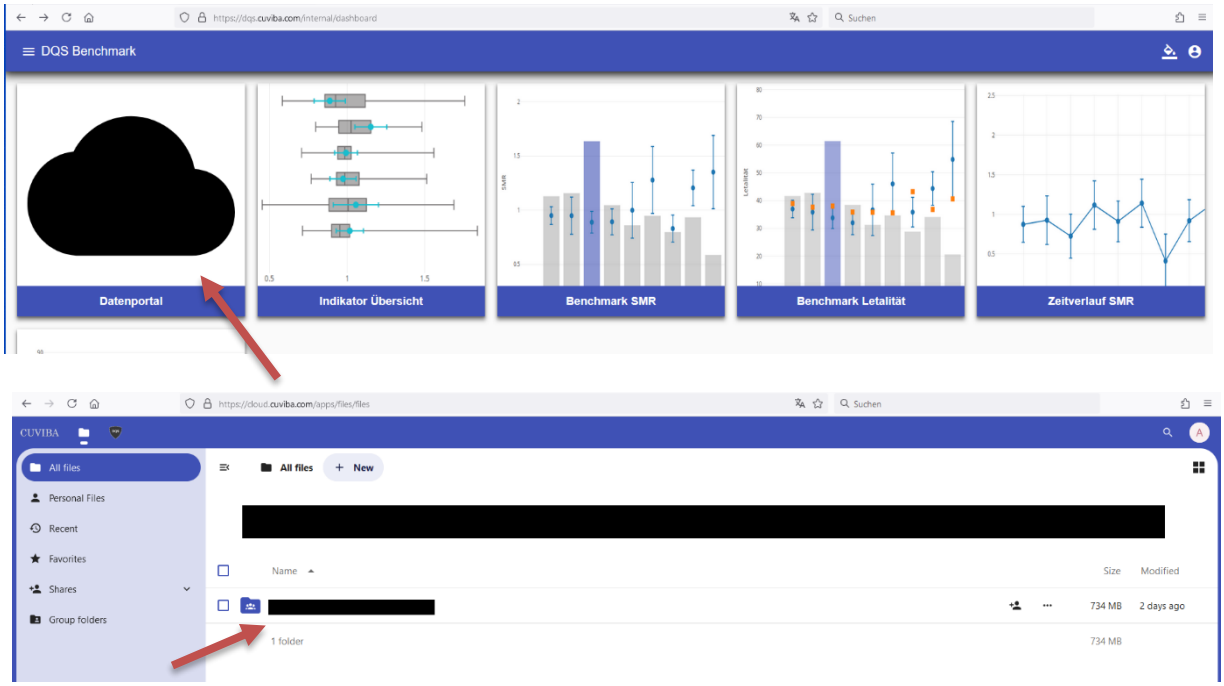


Abbildung 11

Laden Sie die Datei (üblicherweise „einzelfallliste_full_“ gefolgt von dem Name und der cuviba-Kennnummer Ihres Hauses) herunter und speichern Sie diese in Ihrem System. Öffnen Sie nun den CryptoWizard und folgen Sie im Hauptmenü (Abbildung 3) der Schaltfläche „Ergebnislieferung des DQS-IT-Dienstleister entschlüsseln“. Ein neues Fenster öffnet sich (Abbildung 12). **Durchsuchen** Sie Ihre Ordner nach der zuvor gespeicherten Einzelfallliste, die Sie entschlüsseln möchten. Zu entschlüsselnde Dateien sind anhand der .gpg-Endung gut zu erkennen. Klicken Sie anschließend auf „Entschlüsseln“. Der Wizard entschlüsselt

nun Ihre Datei und speichert Sie am gleichen Ort, wo Sie zuvor die verschlüsselte Datei gespeichert haben (Abbildung 13).

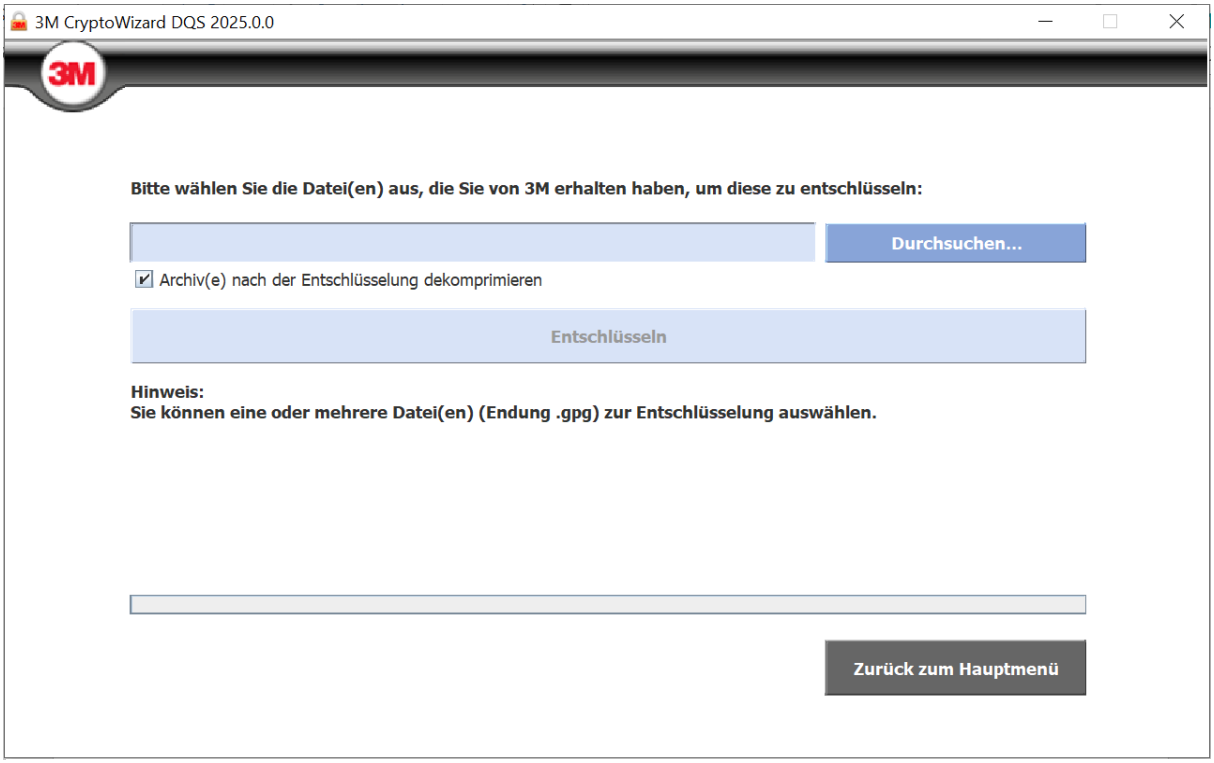


Abbildung 12

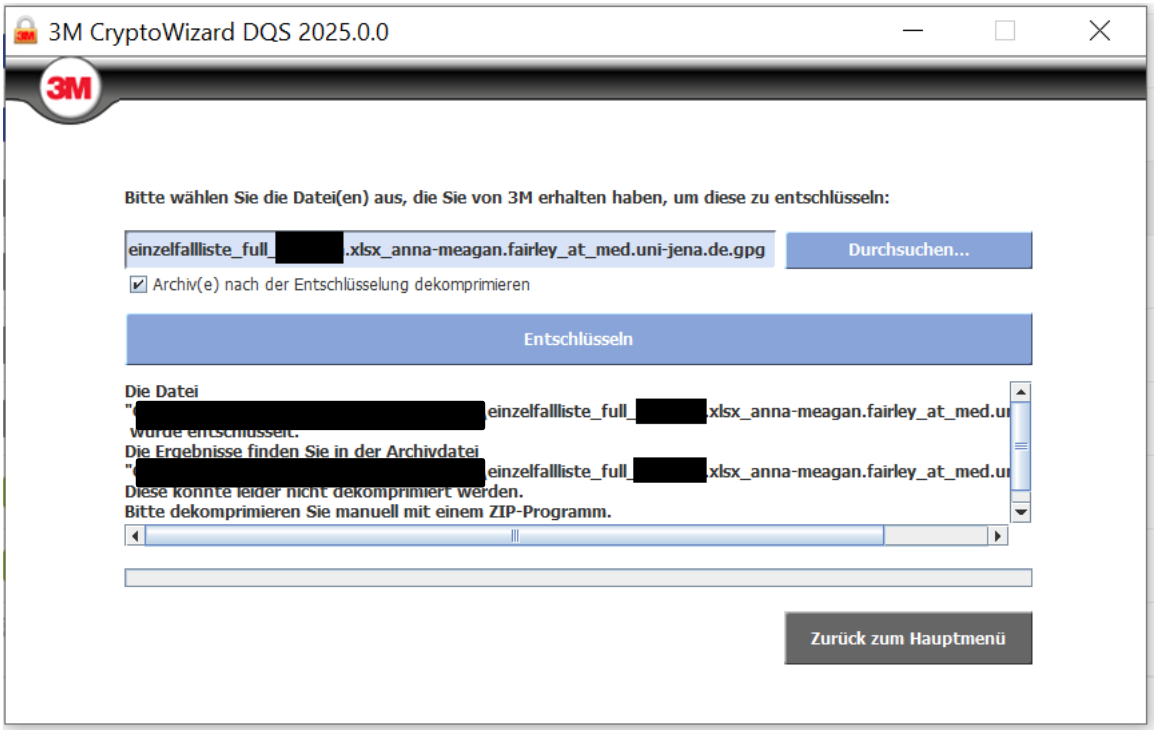


Abbildung 13

HINWEIS: Die Funktion „Archiv(e) nach der Entschlüsselung dekomprimieren“ ist dann relevant, wenn Sie von cuviba eine komprimierte zip-Datei erhalten sollten und entschlüsseln müssen, andernfalls können Sie dies ignorieren. Es schadet nicht, dies einfach markiert zu lassen und Sie können die Fehlermeldung ignorieren.

2.3 Einzelfallliste depseudonymisieren

Für die Depseudonymisierung muss die original krankenhausinterne Fallnummer aus der gespeicherten Mappingdatei (vgl. Abschnitt 1.4.2) an das Pseudonym in der Einzelfallliste angespielt werden. Hierzu können unterschiedlichste Methoden eingesetzt werden (z.B. Datenbanksoftware oder Statistiksoftware). Verwenden Sie also gern diejenige Methode, die Ihnen oder verfügbaren Expert:innen in Ihrem Haus vertraut ist. Sofern keine spezialisierte Software oder Expertise vorliegt, möchten wir Ihnen eine einfache Methode der Depseudonymisierung nahelegen, für die sie lediglich eine aktuelle Version von Microsoft Excel benötigen.

WICHTIG: Für die Depseudonymisierung benötigen Sie Ihre **Mappingdatei** – also die Datei in der die entsprechenden Pseudonyme zu den Fallnummern aus Ihrer **letzten Datenlieferung** gelistet sind. Diese sollte Ihnen aus dem Cryptowizard zur Verfügung stehen. Bitte beachten Sie, dass nur die Mappingdatei der letzten Lieferung für die Depseudonymiserung funktioniert. D.h., Fälle aus älteren Lieferungen, die in der Einzelfallliste enthalten sind, können Sie auch nur mit älteren Mappingdateien der älteren Datenlieferungen depseudonymisieren. Hierfür ist die vorgestellte einfache Excel-Methode jedoch nicht mehr geeignet und Expertise für Datenverarbeitung erforderlich. Kontaktieren Sie im Zweifel das DQS-Koordinationsbüro.

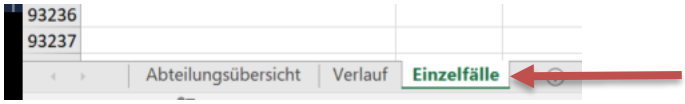
HINWEIS: Die Einzelfallliste ist ein komplexes Excel-Dokument, das aggregierte Betrachtungen über Fachabteilungen und Zeitverläufe für alle Sepsis/Infektionskategorien der DQS-Qualitätsberichte ermöglicht. Hierfür kommen Pivot-Tabellen zum Einsatz. Es sind darum die gleichen Fälle mehrfach in der Einzelfallliste enthalten (jeder Fall für jede Sepsis/Infektionskategorie). Hierbei handelt es sich nicht um einen Fehler, sondern um ein technisches

Erfordernis. Für die inhaltliche Anwendung und Interpretation der Einzelfallliste beachten Sie die gesonderte Anleitung zur Interpretation der Qualitätsberichte.

WICHTIG: Für den reibungslosen Verlauf müssen die Spalten mit den Pseudonymen in ihrer Einzelfallliste und Ihrer Mapping-Datei identisch bezeichnet sein (z.B. „Pseudonym“). Als Standard heißt die Spalte in Ihrer Einzelfallliste „Fallnummer“. Stellen Sie sicher, die Spalte vorher so umzubenennen, das diese und die Spalte in Ihrer Mappingdatei identisch heißen.

Schritt 1

Öffnen Sie Ihre Einzelfallliste in Excel – achten Sie darauf die tatsächliche Liste zu öffnen und nicht die Pivot Tabellen. Sie finden die Liste im Tabelenblatt „Einzelfälle“ am unteren Rand des Fensters.



Im Reiter „Daten“ finden Sie den Punkt „Neue Abfrage“. Im Dropdown-Menü unter „Abfragen kombinieren“ finden Sie den Abfrage-Editor. Öffnen Sie den **Abfrage-Editor** (Abbildung 14).

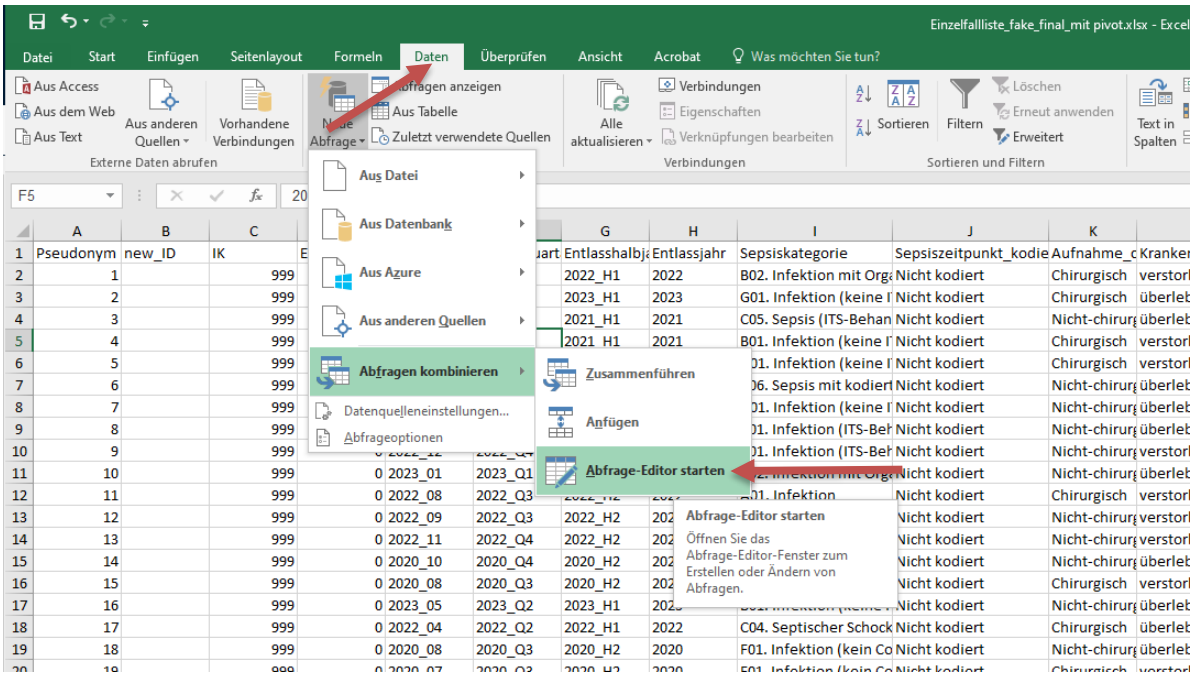
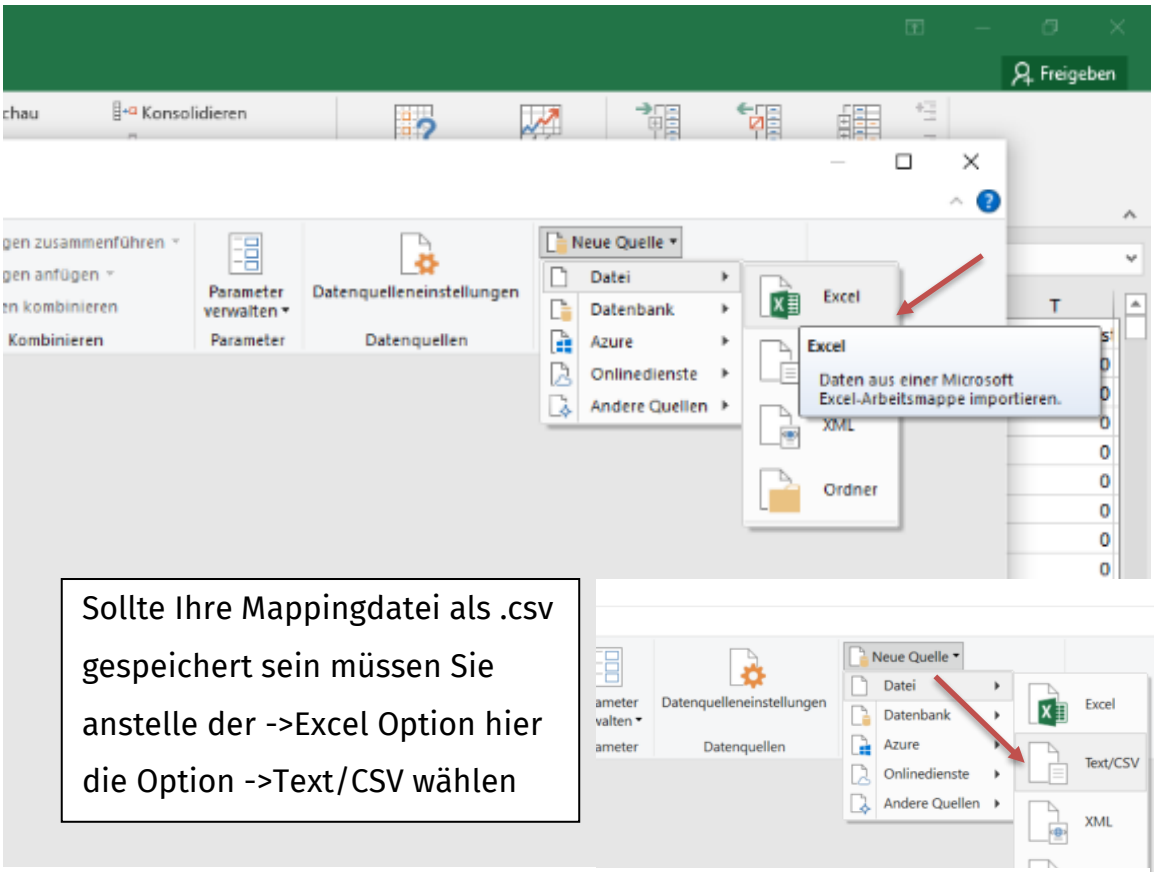


Abbildung 14

Schritt 2

Der Abfrage-Editor öffnet in einem separaten Fenster. Unter „Neue Quelle“ wählen Sie -> Datei -> Excel, und öffnen sie jetzt hier **NOCHMAL** ihre Einzelfallliste (Abbildung 15a).



Sollte Ihre Mappingdatei als .csv gespeichert sein müssen Sie anstelle der ->Excel Option hier die Option ->Text/CSV wählen

Abbildung 15a

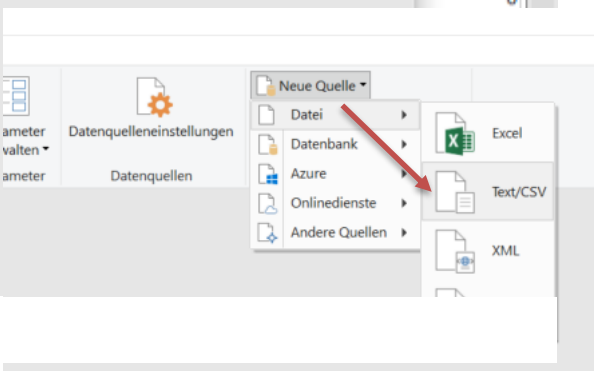


Abbildung 15b

Ein Navigationsfenster erlaubt Ihnen nun auch hier die Auswahl des Tabellenreiters mit der Liste („Einzelfälle“), ignorieren Sie die Reiter mit den Pivot Tabellen (Abbildung 16).

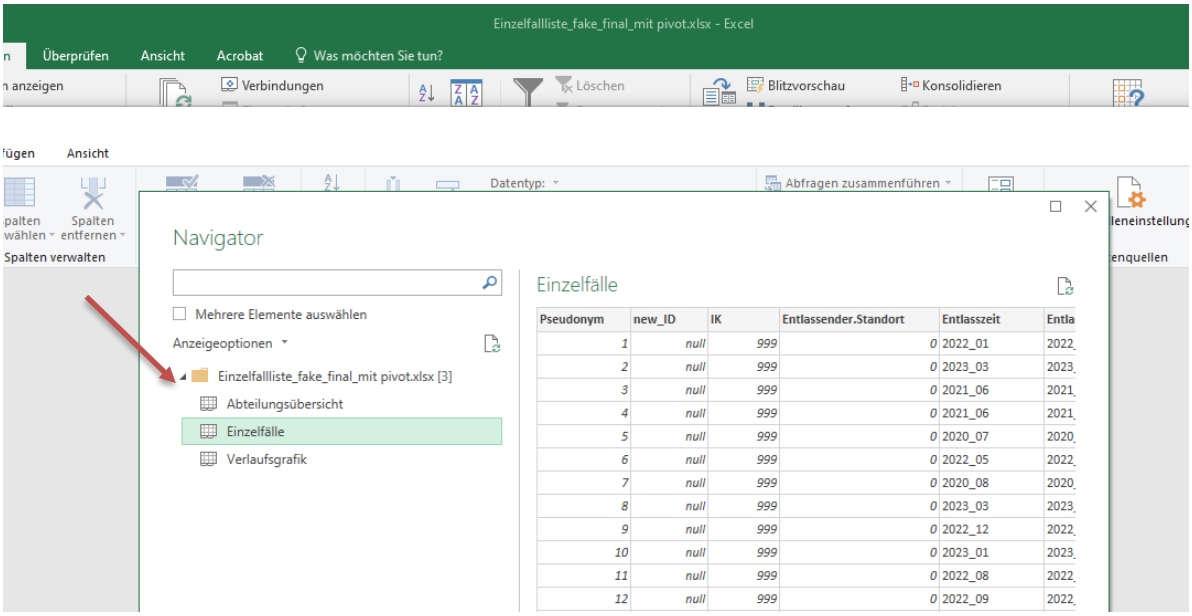


Abbildung 16

In einem zweiten Durchgang öffnen Sie auf die gleiche Weise (Abbildung 15) Ihre Mapping Datei – sollte diese als .csv gespeichert sein müssen Sie anstelle von ->Excel die Option ->Text/CSV wählen, was Ihnen die Möglichkeit gibt .txt und .csv Dateien zu öffnen (Abbildung 15b). Nun sollten beide Tabellen im Abfrage-Editor aufgeführt sein.

Schritt 3

Nun werden die beiden Tabellen zusammengeführt: Klicken Sie unter ‚Kombinieren' auf ‚Abfragen zusammenführen' (Abbildung 17).

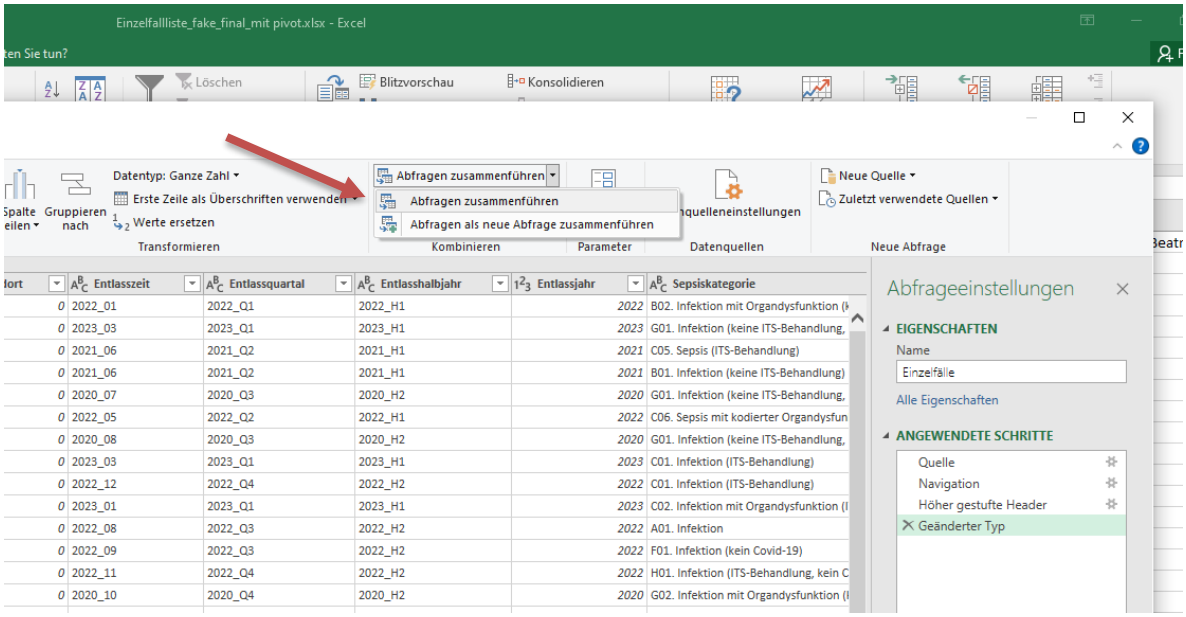


Abbildung 17

Ein Fenster öffnet sich in dem Sie die beiden ausgewählten Tabellen aufgeführt bekommen (Abbildung 18). Wählen Sie die Spalte ‚Pseudonym' in beiden Tabellen aus und wählen Sie die Join-Art „Inner Join (nur übereinstimmende Zeilen)". Bestätigen Sie mit „OK".

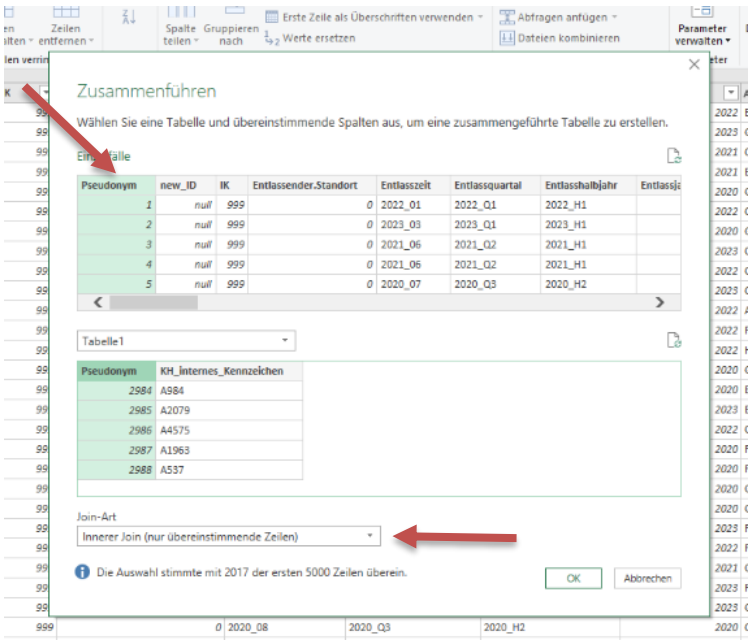


Abbildung 18

Schritt 4

Der Abfrage-Editor ergänzt eine Spalte in der Einzelfallliste (Abbildung 19). Sie müssen hierzu die Spalte angeben die Sie einfügen möchten. Klicken Sie auf das Symbol in der neuen Spalte und wählen Sie den Inhalt aus, der das interne Kennzeichen in die Spalte einfügt (In unserem Beispiel „KH_internes_Kennzeichen“, doch bei Ihnen kann diese Spalte anders heißen.

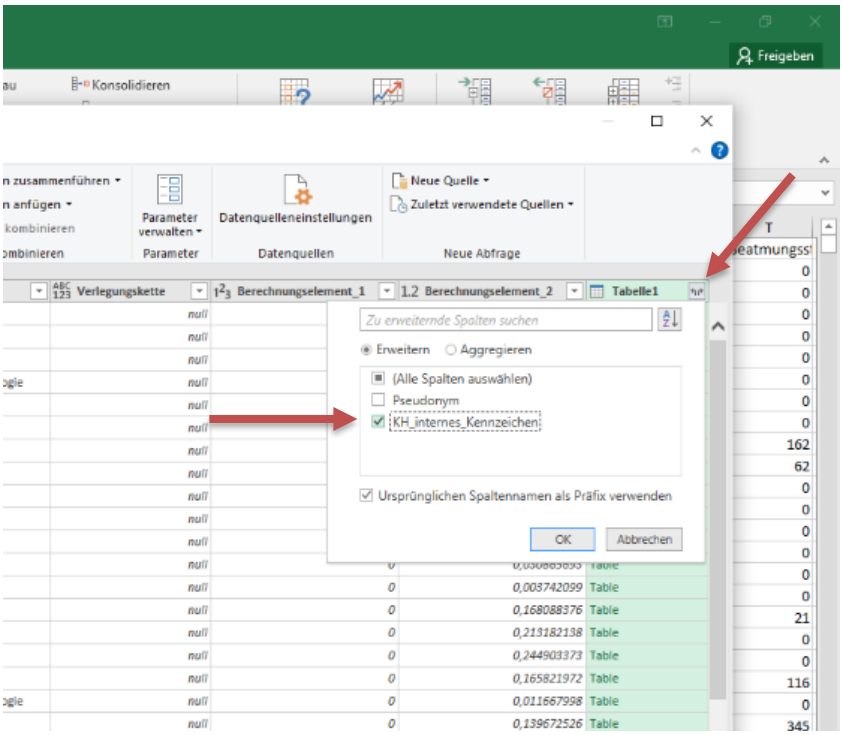


Abbildung 19

Schritt 5

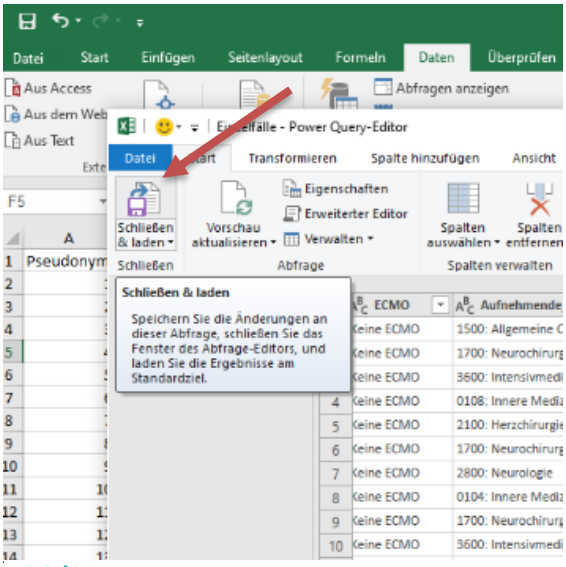


Abbildung 20

Speichern Sie nun die zusammengeführte Abfrage (Abbildung 20). Excel fügt nun der Einzelfallliste zwei neuen Tabellenblätter aus dem Abfrage-Editor hinzu (Abbildung 21). Tabelle1 ist die Einzelfallliste mit depseudonymisierten, internen Kennzeichen (die neue Spalte mit den internen Kennzeichen befindet sich ganz hinten in der Tabelle), Tabelle2 ist Ihre Mapping Datei mit dem Pseudonym und dem dazugehörigen internen Kennzeichen,

Sie können diese Tabelle entfernen. Damit ist Ihre Einzelfallliste depseudonymisiert und kann nun benutzt werden, um konkrete Fälle zu identifizieren.

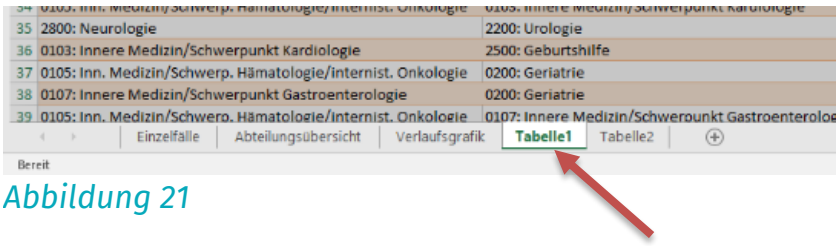


Abbildung 21

Abschließend benennen Sie am Besten dasTabellenblatt "Tabelle1" in "Einzelfallliste_depseudonymisiert" um. Dies vereinfacht es den weiteren Nutzenden.
Bitte behalten Sie das Tabellenblatt mit der unveränderten Einzelfallliste und **<u>löschen Sie dieses nicht</u>** - sonst funktionieren die Pivot-Tabellen für Abteilungsübersicht und Verlaufsgrafik nicht mehr.

Bitte stellen Sie die depsedonymisierte Einzelfallliste den in Ihrem Haus für die Qualitätsanalysen zuständigen Mitarbeitenden zu. Liefern Sie die Einzelfallliste in depseudonymisierter Form nicht an unberechtigte Dritte, auch nicht an das DQS-Koordinationsbüro oder cuviba.

3 Anhang

3.1 Anhang 1

Datei §21	Datenfeld	Operation im Normalbetrieb
FALL	KH-internes-Kennzeichen	Austausch der Original-Fallnummer gegen Pseudonym
FALL	Versicherten-ID	Inhalt wird entfernt
FALL	Vertragskennzeichen-64b-Modellvorhaben	Inhalt wird entfernt
FALL	IK-der-Krankenkasse	Inhalt wird reduziert (Übernahme der ersten beiden Stellen, dann folgen "0000000")
FALL	Geburtsmonat	Inhalt wird entfernt
FALL	PLZ	Inhalt wird entfernt
FALL	Aufnahmegewicht	Inhalt wird verändert (Wert wird in 25er-Schritten gerundet)
FALL	Patientennummer	Austausch der Original-Patientennummer gegen Pseudonym
FALL	Behandlungsbeginn-vorstationär	Inhalt wird entfernt
FALL	Behandlungstage-vorstationär	Inhalt wird entfernt
FALL	Behandlungsende-nachstationär	Inhalt wird entfernt
FALL	Behandlungstage-nachstationär	Inhalt wird entfernt

FALL	IK-Verlegungs-KH	Inhalt wird entfernt
FALL	Belegungstage-in-anderem-Entgeltbereich	Inhalt wird entfernt
FALL	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt
FAB	KH-internes-Kennzeichen	Austausch der Original-Fallnummer gegen Pseudonym
FAB	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt
ICD	KH-internes-Kennzeichen	Austausch der Original-Fallnummer gegen Pseudonym
ICD	Diagnosesicherheit	Inhalt wird entfernt
ICD	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt
OPS	KH-internes-Kennzeichen	Austausch der Original-Fallnummer gegen Pseudonym
OPS	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt
Entgelte	KH-internes-Kennzeichen	Austausch der Original-Fallnummer gegen Pseudonym
Entgelte	IK-Krankenkasse	Inhalt wird reduziert (Übernahme der ersten beiden Stellen, dann folgen "0000000")
Entgelte	Entgeltart	mit 4 beginnend gelöscht
Entgelte	Entgeltbetrag	auf 0 gesetzt
Entgelte	Abrechnung-von	Inhalt wird entfernt
Entgelte	Abrechnung-bis	Inhalt wird entfernt
Entgelte	Tag-der-Behandlung	Inhalt wird entfernt

Entgelte	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt

Alle hier nicht aufgeführten Felder bleiben unverändert. (Felder, die nicht Teil einer § 21-Datensatzspezifikation sind, werden vollständig entfernt.)

Deutsches
Qualitätsbündnis
SEPSIS