Kurzgutachten

Zeitpunkt der Prüfung

Die Prüfung des Verfahrens fand vom 17.10.2013 bis zum 02.09.2015 statt.

Adresse des Antragstellers

AQUA - Institut für angewandte Qualitätsförderung
und Forschung im Gesundheitswesen GmbH
Maschmühlenweg 8 – 10
37073 Göttingen

Kurzbezeichnung des Produkts/Verfahrens

„AQUA SQG" - Externe (sektorenübergreifende) Qualitätssicherung

Adresse der Sachverständigen

Andreas Bethke
Dipl. Inf. (FH)
Papenbergallee 34
25548 Kellinghusen
email: beth-ke@datenschutzguetesiegel.sh

Stephan Hansen-Oest
Rechtsanwalt & Fachanwalt für IT-Recht
Neustadt 56
24939 Flensburg
email: sh@datenschutzfreundlich.de

Detaillierte Bezeichnung des Begutachtungsgegenstandes

Der Anbieter führt Qualitätssicherungsanalysen im Gesundheitswesen durch. Rechtsgrundlage für die Qualitätssicherungsaufgaben, die der Anbieter des Verfahrens mit dem Zertifizierungsgegenstand durchführt, ist § 137a SGB V.

Der Verfahrensanbieter hat in umfangreichen Recherchen, Untersuchungen und Dokumentationen die Qualitätsindikatoren für eine Überprüfung der Qualität in der Gesundheitsversorgung definiert (dokumentiert hier: „Allgemeine Methoden im Rahmen der sektorenübergreifenden Qualitätssicherung im Gesundheitswesen nach §137a SGB V - Version 3.0").

Nach der Definition des Anbieters ist Qualitätssicherung die Summe aller Maßnahmen, die geplant und systematisch eingesetzt werden, um definierte Qualitätsanforderungen zu überprüfen, sicherzustellen bzw. sie zu erreichen.
Der Datenfluss bei der Erhebung von Qualitätsdaten, deren Auswertung und Berichterstattung sieht wie folgt aus:

Datenannahme
Das Verfahren der Datenannahme und –auswertung ist in der QSKH-RL und der Qesü-RL geregelt. Alle Leistungserbringer (also z. B. Krankenhäuser, medizinische Versorgungszentren etc.) übermitteln ihre Qualitätssicherungsdaten an sog. „Datenannahmestellen". Für Ärzte ist diese in der Regel die zuständige Kassenärztliche Vereinigung (KV) bzw. Kassenzahnärztliche Vereinigung (KZV). Datenannahmestelle für Krankenhäuser ist die jeweilige Landesgeschäftsstelle für Qualitätssicherung (LQS) oder die jeweilige Landeskrankenhausgesellschaft (LKG). Diese und weitere Zuständigkeiten für Datenannahmestellen sind in § 16 QSQKH-RL und § 9 Abs. 1 Qesü-RL geregelt.

Nach § 9 Abs. 2 Qesü-RL prüfen die Datenannahmestellen die übermittelten Daten auf Plausibilität, Vollständigkeit und Vollzähligkeit, soweit dies mit den datenschutzrechtlichen Vorgaben des § 299 Abs. 1 Satz 7 SGB V vereinbar ist.

Die Details der Verschlüsselung bei der Annahme der Daten sind ebenfalls in der „Anlage zu Teil 1" Qesü-RL in § 3 Abs. 3 sowie in dem seriellen Datenflussmodell, das als Abbildung 1 der Qesü-RL beigefügt ist, geregelt.

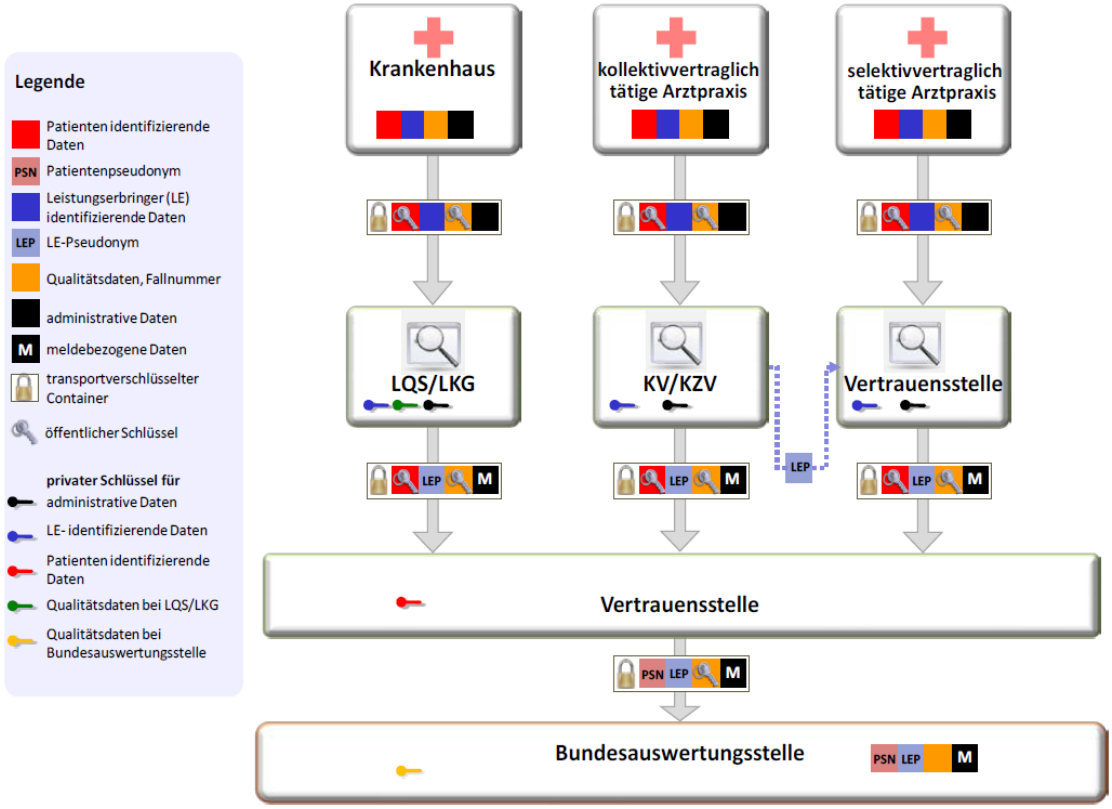

Abbildung 1 - Datenflussmodell der Qesü-RL

Im Zusammenhang mit der Datenerhebung gemäß QKSH-RL ist grundsätzlich nach vier verschiedenen Datenarten zu differenzieren:

1. Qualitätssicherungsdaten
2. Jährliche Sollstatistik
3. Benchmark-Reports
4. Datum zum Strukturierten Dialog und für die Qualitätsberichte (in Verbindung mit der Qb-R des G-BA)

Die Qualitätssicherungsdaten (1.) werden ausschließlich verschlüsselt übertragen.

Bei der Verschlüsselung muss generell zwischen der XML- Encryption und der Transportverschlüsselung unterschieden werden:

Der Anbieter verwendet XML-Encryption, um unterschiedliche Dokumentenabschnitte (XML-Knoten) für unterschiedliche Datenempfänger mit unterschiedlichen, öffentlichen Schlüsseln zu verschlüsseln. Auf diese Weise ist jeder verschlüsselte Dokumentenabschnitt nur für den Besitzer des jeweiligen Schlüssels lesbar.

Für die Verschlüsselung der XML-Knoten wird die hybride Verschlüsselung nach dem W3C-Standard „XML Encryption Syntax and Processing" verwendet. Im Detail erfolgt die Verschlüsselung zunächst mit einem zufällig erzeugten, symmetrischen Schlüssel, der wiederum mit dem Public Key der zuständigen Datenannahmestelle verschlüsselt wird. Als Verschlüsselungsalgorithmen werden „AES128" für die symmetrische Verschlüsselung der XML-Elemente und „RSA mit 2048-Bit" für die asymmetrische Verschlüsselung des generierten symmetrischen Schlüssels verwendet.

Für die zusätzliche Transportverschlüsselung zwischen den Beteiligten den Krankhäusern (KH) , Datenannahmestelle auf Landesebene (DAS), Vertrauensstelle (VST) sowie der Bundesauswertungsstelle (BAS) wird noch einmal die gesamte XML-Datei gepackt und verschlüsselt.

Das Einmelden geschieht via E-Mail. Die E-Mails werden automatisiert verarbeitet (Speicherung des verschlüsselten Anhangs zur weiteren Verarbeitung) und in ein revisionssicheres E-Mail-Archiv verschoben.

Schlüsselmanagement
Auf Landesebene erstellt die Datenannahmestelle (DAS) einen privaten und einen öffentlichen Schlüssel. Der öffentliche Schlüssel wird den Leistungsempfängern (LE) und SWA zur Verfügung gestellt. Zusätzlich erhält das AQUA-Institut von allen DAS die öffentlichen Schlüssel, und stellt sie als ein Schlüsselpaket allen Softwareanbietern (SWA) auf der SQG-Webseite zur Verfügung.

Nur die Länder besitzen die privaten Schlüssel und können die QS-Daten entschlüsseln. Darüber hinaus besitzt die Vertrauensstelle (VST) für die (patientenidentifizierenden Daten) PID- und die Bundesauswertungsstelle (BAS) für die direkten Verfahren und für die verschlüsselte Datenübertragung zwischen den Datenannahmestellen und AQUA eigene öffentliche Schlüssel.

Bei den Daten, die von Arztpraxen, MVZ und Belegärzten gemäß der Qesü-RL an die KV zu übermitteln sind, ist von den Betroffenen anstelle des öffentlichen Schlüssels der Landesebene derjenige der Bundesauswertungsstelle zu verwenden, da die KV als DAS keinen Einblick in die QS-Daten erhalten darf.

Im Falle einer Kompromittierung eines Schlüssels werden neue Schlüssel generiert. Der neue öffentliche Schlüssel wird auf der Webseite veröffentlicht und die betroffenen Datenlieferanten werden darüber informiert.
Sollte ein Datenlieferant nach dem Austausch der Schlüssel durch AQUA die alten Schlüssel weiter verwenden, bekäme er im Protokoll unverzüglich eine Fehlermeldung.

In datenschutzrechtlicher Hinsicht ist von Bedeutung, dass aufgrund der verwendeten Verschlüsselung eine Personenbeziehbarkeit der Daten für AQUA als Verfahrensanbieter ausgeschlossen ist. Zugriff besteht nur auf Vorgangsnummern. Die Vorgangsnummern müssen in den Qualitätsdaten enthalten sein, weil nur auf dieser Basis bei Bedarf Rückfragen im Krankenhaus z. B. zu Auffälligkeiten möglich sind. Sie dienen aber nur zur Identifizierung von Datensätzen. „Personenbeziehbar" ist die Vorgangsnummer nur innerhalb des speziellen Softwaresystems im Krankenhaus, wenn die Vorgangsnummer mit weiteren krankenhausinternen Informationen verknüpft wird, nicht jedoch für AQUA als Verfahrensanbieter.

Die jährliche Sollstatistik (2.) wird per E-Mail versendet. Hier kommt ebenfalls eine Transportverschlüsselung zum Einsatz, wobei ein PGP-Verfahren zur Anwendung kommt.

Die Benchmark-Reports (3.) hingegen werden über die Internetseite des Verfahrensanbieters (via sqg.de) übermittelt. Die Benchmark-Reports enthalten keine personenbezogenen Daten und werden von z. B. den Krankenhäusern nach einer erfolgten Anmeldung via Benutzername/Passwort an den Verfahrensanbieter über eine SSL-verschlüsselte Verbindung übertragen.

Auch die Daten des strukturierten Dialogs und für die strukturierten Qualitätsberichte (4.) werden über die Internetseite des Verfahrensanbieters über eine HTTPS-Verbindung übertragen.

Im Bereich der Daten, die nach der Qesü-RL erhoben werden, erfolgt die Übertragung der Daten im XML-Format. Dabei kommt eine AES 128bit Transportverschlüsselung zum Einsatz. Darüber hinaus werden aber die patientenidentifizierenden Daten und die Qualitätssicherungsdaten separat mit dem AES-Algorithmus verschlüsselt.

Datenauswertung

Im Rahmen des Vergabeverfahrens nach § 137a SGB V ist derzeit der Anbieter des Verfahrens als Bundesauswertungsstelle i.S.d. §§ 7 und 10 Abs. 2 Qesü-RL tätig. Aufgaben der Auswertungsstelle sind nach den Vorgaben von § 10 Abs. 2 Qesü-RL und § 8 QKSH-RL:

- die Überprüfung der übermittelten Datensätze auf Vollzähligkeit, Vollständigkeit und Plausibilität,
- die patientenbezogene Zusammenführung von Daten und deren Überprüfung,
- die Rückspiegelung der Auswertungen an die Landesarbeitsgemeinschaften (indirekte Verfahren) bzw. die datenübermittelnden Stellen (direkte Verfahren) (Rückmeldeberichte),
- die Vorhaltung der geprüften Daten,
- die Übermittlung angeforderter Auswertungen an den G-BA.

Die Details der Datenauswertung sind im Einzelnen nicht Gegenstand der Zertifizierung. Gegenstand der Zertifizierung ist die Auswertung nur insoweit, dass nachgeprüft wird, dass aus den Daten kein Personenbezug für Dritte herzuleiten ist.

Datenvalidierung

Ähnlich wie bei der Datenauswertung prüft das Verfahren des Anbieters auch die Validität der übermittelten Daten der Qualitätssicherung. Rechtsgrundlage für die Datenvalidierung ist § 9 QSKH-RL. Die insoweit durchgeführte Validierung lässt sich dem Ablauf nach der nachfolgenden Abbildung entnehmen:

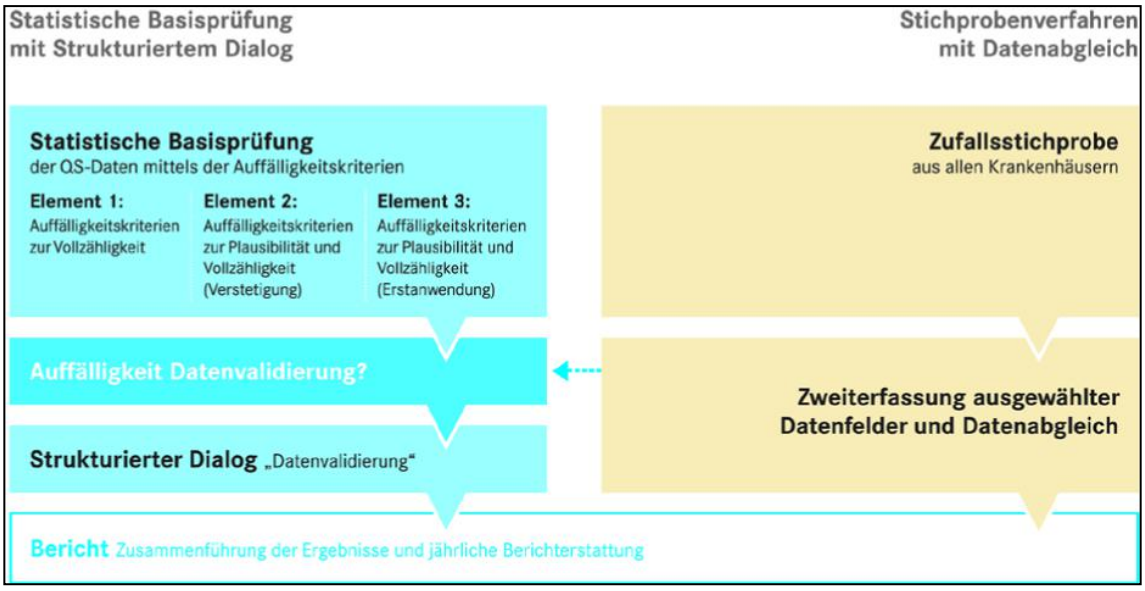

Abbildung 2 - Datenvalidierung

Wie bei der Datenauswertung ist auch die Datenvalidierung nicht vollständig Gegenstand der Zertifizierung. Der Untersuchungsgegenstand beschränkt sich insoweit auf den Umstand, dass nur geprüft worden ist, ob aus den zu validierenden Daten ein Personenbezug zu ermitteln ist.

Sonstiges

Im Zusammenhang mit der Durchführung des Verfahrens kann es zu E-Mail-Kommunikation mit beteiligten Personen anderer Stellen kommen. Diese E-Mails enthalten keine Daten über Patienten o. Ä. Die E-Mails werden (ebenso wie die E-Mails mit einliefernden Daten wie oben beschrieben) archiviert; da auch die Angaben zu Absender und Empfänger personenbezogene Daten sein können, wird darauf hingewiesen, dass die Software zur E-Mail-Archivierung nicht Gegenstand der Zertifizierung ist. Gleiches gilt für eine etwaige Verarbeitung von Nutzungs- oder Bestandsdaten der Internetseite des Anbieters des Verfahrens. Auch diese ist nicht Gegenstand der Zertifizierung.

Zusammenfassung und Abgrenzung des Zertifizierungsgegenstands

Die Zertifizierung beschränkt sich auf folgende Tätigkeiten und Leistungen, die vom AQUA-Institut erbracht werden:

- die Schlüsselgenerierung für den verschlüsselten Austausch zwischen den Datenannahmestellen (DAS) und der Bundesauswertungsstelle (BAS), also dem

AQUA-Institut selbst, sowie dem verschlüsselten Austausch zwischen der Vertrauensstelle (VST) und der BAS,

- die Datenannahme (s. Abbildung 3: Datenservice),
- Teile der Datenauswertung (s. Abbildung 3 - Datenfluss: Datenauswertung)
    - Überprüfung der übermittelten Datensätze auf Vollzähligkeit, Vollständigkeit und Plausibilität
    - patientenbezogene Zusammenführung von Daten und deren Überprüfung
    - Rückspiegelung der Auswertungen an die Landesarbeitsgemeinschaften bzw. die datenübermittelnden Stellen (Rückmeldeberichte)
    - Vorhaltung der geprüften Daten
    - Übermittlung angeforderter Auswertungen an den G-BA
- Teile der Datenvalidierung (Prüfung, ob ein Personenbezug herstellbar ist).

Zweck und Einsatzbereich des Begutachtungsgegenstandes

Zweck des Verfahrens ist die Durchführung von Qualitätsuntersuchungen im Zusammenhang mit der Erbringung von medizinischen Leistungen im Rahmen der Gesundheitsversorgung. Dabei wird durch die Verwendung von Qualitätsindikatoren bei medizinischen Einrichtungen, insbesondere Krankenhäusern, eine Erhebung von Daten durchgeführt. Da es sich bei einem Krankenhaus auch um eine öffentliche Stelle des Landes Schleswig Holsteins handeln kann, ist dieses Verfahren grundsätzlich auch für den Einsatz bei öffentlichen Stellen des Landes Schleswig-Holstein geeignet.

Modellierung des Datenflusses

Abbildung 3 - Datenfluss

Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog Version 1.2

Zusammenfassung der Prüfungsergebnisse

Bei dem Verfahren des Anbieters werden die Patientendaten im Zusammenhang mit der Datenannahme pseudonymisiert, so dass der Anbieter des Verfahrens bzw. die jeweilige Datenannahmestelle keinen Personenbezug aus den Daten herleiten kann.

Für diese Stellen besteht insoweit kein Personenbezug. Der Verfahrensanbieter kann aus den Daten keinen Personenbezug herleiten, insbesondere ist eine De-Pseudonymisierung nicht möglich. Eine „unbefugte" Offenbarung i.S.d. § 203 StGB liegt zudem nicht vor, da § 299 SGB V die pseudonyme Übertragung von Daten, die auch einer Schweigepflicht unterliegen können, vorsieht und insoweit eine Rechtsgrundlage für die „Offenbarung" vorliegt.

Für die Verarbeitung von Daten im Zusammenhang mit der Qualitätssicherung im Gesundheitswesen gibt es bereichsspezifische Rechtsgrundlagen im SGB V. Nach § 299 SGB V sind die Leistungserbringer der medizinischen Versorgung befugt und verpflichtet, personenbezogene Daten für Zwecke der Qualitätssicherung zu erheben, verarbeiten oder zu nutzen, soweit dies nach den Richtlinien des G-BA vorgesehen ist.

Art und Umfang der Datenverarbeitung richten sich im Falle des Untersuchungsgegenstandes konkret nach den Richtlinien des G-BA. Der Datenfluss ist konkret in der Qesü-RL vorgegeben.

Die Richtlinien des G-BA stellen im Zusammenhang mit § 299 SGB V eine ausreichende Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Zusammenhang mit dem Untersuchungsgegenstand dar.

Die Speicherdauer der eingelieferten und verarbeiteten Daten ist auf maximal 3 Jahre beschränkt. Dies bezieht sich auch auf archivierte E-Mails.
Soweit der Anbieter Daten verarbeitet, erfolgt dies in einem eigenen Rechenzentrum. Das Rechenzentrum erfüllt alle Anforderungen an die Datensicherheit, insbesondere im Hinblick auf die technischen und organisatorischen Maßnahmen i.S.d. Anlage zu § 9 Satz 1 BDSG als auch den technischen Anforderungen des Kriterienkataloges für das Gütesiegel für IT-Produkte.

Der Zugang zu IT-Systemen und Applikationen, die im Zusammenhang mit dem Zertifizierungsgegenstand zum Einsatz kommen, ist in vorbildlicher Weise umgesetzt. Es gibt insbesondere gute Richtlinien im Umgang mit Passwörtern und für den Umgang mit Daten.

Im Rahmen der Verfügbarkeitskontrolle werden täglich automatische Datensicherungen auf den Servern in den Abendstunden durchgeführt.

Die Datenverarbeitung mit dem Verfahren "AQUA SQG" kann bei einem Einsatz in öffentlichen Stellen in datenschutzkonformer Weise erfolgen.

Durch die verwendeten Verschlüsselungstechnologien wird insbesondere eine Kenntnisnahme von Patientendaten durch den Anbieter des Verfahrens unterbunden.

Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das Produkt verwendet Pseudonymisierungstechnologien in vorbildlicher Weise. Die Pseudonymisierung erfolgt in einem sehr frühen Stadium, so dass gewährleistet ist, dass keiner der Verfahrensbeteiligten und insbesondere nicht der Anbieter des Verfahrens Kenntnis von unmittelbar personenbezogene Daten erhält. Lediglich die Vorgangsnummern werden beim Anbieter des Verfahrens vorgehalten. Der Anbieter selbst kann aus diesen Vorgangsnummern jedoch keinen Personenbezug herleiten. Die Vorgangsnummern sind zum einen für die Datenauswertung und zum anderen für die Kommunikation mit der einliefernden Stelle (Krankenhäuser) erforderlich, um im Einzelfall Überprüfungen vorzunehmen.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den 17.11.2015

Andreas Bethke

Flensburg, den 17.11.2015

Stephan Hansen-Oest