Technisches und rechtliches Rezertifizierungs-Gutachten

Einhaltung datenschutzrechtlicher Anforderungen durch das Produkt „Elefant Profi Version 13.02“ der

HASOMED GmbH
Magdeburg

erstellt von:

Stand:
Mai 2013

Inhaltsverzeichnis

Änderungs- und Versionsverwaltung des Gutachtens

01.10.2012	Erstellung	
10.10.2012	Ergänzung	
19.10.2012	Überarbeitung	
05.11.2012	Ergänzung	
02.05.2013	Überarbeitung	
23.05.2013	Letzte Korrekturen	

A. Einleitung

1 Mit dem vorliegenden Gutachten beabsichtigt die HASOMED GmbH (nachfolgend HASOMED genannt) ihr Produkt „Elefant Profi“ mit der Option „Security Mode“ für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) rezertifizieren zu lassen.

Die Vorlage des Gutachtens beim ULD erfolgt durch den Auftraggeber.

Dem Gutachten wird der Anforderungskatalog in der Version 1.2 zu Grunde gelegt.

2 HASOMED möchte mit diesem Gutachten den Nachweis führen, dass das Produkt mit den Änderungen und Neuerungen, die seit der Erteilung des Gütesiegels vom 12.12.2007 und der Rezertifizierung vom 18.05.2010 gemacht worden sind, nach wie vor die datenschutzrechtlichen Anforderungen erfüllt.

B. Zeitpunkt der Prüfung

3 Die Prüfung des Produktes fand vom 05.09.2012 - 02.05.2013 statt.

C. Änderungen und Neuerungen des Produktes

4 Das Produkt „Elefant Profi“ mit der Option „Security Mode“ wurde um folgende Funktionen erweitert:

- Datenbank anonymisieren
- Erweiterung um eine Schnittstelle für „AMBO“-Abrechnung
- Einbindung von Schnittstellen zu neuen Kartenlesegeräten
- Ermöglichung von zusammenführen von Patientendaten
- Erweiterung der Protokollfunktion im „Security Mode“
- Implementierung der VERAX-Liste
- Implementierung einer Schnittstelle zu Microsoft Outlook zum Verschicken von E-Mails und zur Befüllung von Terminkalendern

Ebenfalls wurde das Programm um eine Schnittstelle zu einem Klinikinformationssystem (kurz KIS) erweitert. Dies ist jedoch nicht Bestandteil des Gütesiegels.

1. Anonymisierung der Datenbank

5 Eine typische Anforderung an den Support von Softwareherstellern im Allgemeinen und Hasomed im Speziellen ist die Behebung von Datenbankproblemen die eine genauere Analyse der Datenbank selbst erforderlich machen, wenn das Problem telefonisch nicht zu beheben ist. Dies können z. B. Inkonsistenzen nach einem Stromausfall sein. Unter diesem Aspekt muss die Datenbank des Kunden zu HASOMED geschickt werden. Da mit dem „Elefanten“ sensible Daten verarbeitet werden, dürfen diese vom Psychotherapeuten aus der Hand gegeben werden. Hierfür wurde eine sog. „Anonymisierungsfunktion“ entwickelt, die durch die gesamte Datenbank geht und dort alle den Patienten kennzeichnenden individuellen Daten derart verändert, so dass eine Zuordnung der zum Patienten erfassten Informationen zu einem Patienten nicht mehr möglich ist. Dies erfolgt so, dass für

jeden Patienten für den Vornamen, Namen, Straße und Ort der Feldbezeichner (also „Vorname“, „Nachname“ usw.) gefolgt von einer fortlaufenden Nummer ersetzt wird. Die Mitgliedsnummer der Krankenkasse wird durch eine Zufallszahl ersetzt und das Geburtsdatum wird stochastisch um einen definierten Wert nach oben und unten verändert, so dass keine groben Altersänderungen auftreten. Diese Vorgehensweise ist wichtig, da die Erfassung von Leistungen altersbezogen erfolgt und damit keine Fehler bei der Vertauschung der Daten für die KV-Abrechnung erzeugt werden dürfen. Da darüber hinaus in abgespeicherten Dateien Klartext zum Patienten existiert, werden diese Dateien durch eine chiffrierte Ziffernfolge ersetzt. Die so anonymisierte Datenbank kann dann komprimiert an HASOMED übermittelt werden. Die Anonymisierung erfolgt dabei nicht auf dem Originaldatenbestand. Das Programm legt automatisch ein Backup an. Hierauf wird der Benutzer in einem Dialog hingewiesen.

2. Erweiterung um eine Schnittstelle für „AMBO“-Abrechnung

6 Diese Erweiterung hat einen gesetzlichen Hintergrund: Die Abrechnung der psychiatrischen Institutsambulanzen nach §118 SGB V muss seit dem 01.07.2010 über den Datenträgeraustausch nach §301 SGB V vorgenommen werden. Hierzu wurde zwischen der Deutschen Krankenhausgesellschaft (DKG) und dem GKV-Spitzenverband eine Vereinbarung nach § 120 Abs. 3 SGB V über Form und Inhalt der Abrechnungsunterlagen für die Einrichtungen nach §§ 117 bis 119 SGB V geschlossen. Danach ist, zusätzlich zu den bisherigen papiergebundenen Rechnungen, eine elektronische Datenübermittlung notwendig.

Der „Elefant“ wurde um diese Schnittstelle erweitert. Die Übertragung der AMBO-Daten selbst erfolgt dabei verschlüsselt nach einem der AMBO-Spezifizierung folgenden Schlüssel (PKCS #7). Die für AMBO im Datenverzeichnis des Elefanten archivierten Daten werden beim Security-Mode mit dem internen Security-Schlüssel verschlüsselt und können nur über den Elefanten wieder ausgelesen werden.

3. Einbindung von Schnittstellen zu neuen Kartenlesegeräten

7 Da immer neue Kartenlesegeräte auf den Markt kommen, die im Zuge von neuen Versichertenkarten (Gesundheitskarte) hergestellt werden, muss sich der Hersteller den Gegebenheiten des Marktes anpassen und sein Produkt um Schnittstellen zu der neuen Hardware erweitern.

4. Ermöglichung von zusammenführen von Patientendaten

8 Wird ein Patient versehentlich zwei Mal im System angelegt, so wird u. U. nicht nur die Datenintegrität verletzt, sondern auch die Forderung nach Datenvermeidung und Datensparsamkeit. Da eine manuelle Zusammenführung wiederum fehlerbehaftet sein kann, unterstützt der „Elefant“ die automatische Zusammenführung. Bei einer solchen Zusammenführen mehrerer Datensätze von Patienten zu einem Datensatz erfolgt ein Protokolleintrag im Security-Mode derart, dass auf die Zusammenfügung verwiesen wird. Bei

der Zusammenführung dieser Datensätze werden alle Patientendatensätze dem Zielpatienten zugeordnet. Bei Krankenakten ist eine solche automatische Zusammenführung nicht möglich ist, so dass der Benutzer die Daten per Drag & Drop von einer Akte in die andere Akte übertragen muss. Hierfür wird die Systemzwischenablage benutzt, die mit Beenden des Elefanten gelöscht wird, so dass keinerlei Rückstände mit personenbezogenen Daten im System verbleiben.

5. Erweiterung der Protokollfunktion im „Security Mode“

9 Zur Überprüfung der im „Security Mode“ erzeugten Protokolle, die den Vorgaben des LDSG Schleswig-Holstein entsprechen wurde die Protokollfunktion erweitert. D. h. es können nun selektiv Protokolleinträge zu einzelnen Patienten angezeigt werden. Ist ein Patient gelöscht worden, befindet sich in den Protokolleinträgen nur noch der Eintrag, dass der Patient gelöscht wurde. Wird dieser Eintrag nun markiert, kann er nach Rückfrage endgültig gelöscht werden. Damit ist die Anforderung an § 6 Abs. 4 LDSG 2012 erfüllt.

6. Implementierung der VERAX-Liste

10 Die sog. VERAX-Liste ist ein fortlaufend aktualisiertes Verzeichnis aller gesperrten Krankenkassen-Chipkarten, die regelmäßig in die Praxisprogramm der Arztpraxen überspielt werden kann. Wird eine Karte durch das Lesegerät gezogen, so erscheint sofort die Meldung, ob der Versicherte mit dieser Karte versichert ist. Somit soll möglichem Betrug vorgebeugt werden. Der Elefant kann in der vorliegenden Version dieses Verzeichnis einlesen und verarbeiten. Die Verarbeitung erfolgt rein Dateibasiert. Es gibt weder eine Online Abfrage gesperrter Karten durch den Elefant, noch gibt es eine Rückinformation an VERAX und auch keine Statistik im Produkt.

11 Die Liste wird als verschlüsselte Datei abgelegt und Zugriff erfolgt direkt über die DLL mit Übergabe eines Passwortes, welches sich pro Quartal ändert. Die Liste wird einmal im Quartal über das Quartalsupdate aktualisiert.

7. Schnittstelle zu Microsoft Outlook

12 Es wurde eine Schnittstelle zu Microsoft Outlook implementiert, die zum Verschicken von E-Mails (an den Hersteller) und zur Befüllung von Terminkalendern dient. E-Mails können aus verschiedenen Gründen aus dem System heraus verschickt werden. Dabei werden jedoch nie Patientendaten integriert. Es geht hierbei immer um Information der Hotline zu bestimmten Sachverhalten. Die Funktion im Elefanten wird durch eine Schaltfläche neben dem E-Mail-Feld aktiviert. Bevor Outlook gestartet wird, erscheint ein Hinweis für den Therapeuten, dass dieser seinen Patienten über die Risiken einer E-Mail-Nutzung aufklärt und sich eine explizite Einwilligung des Patienten einholt.

Bei der Befüllung des Outlook-Terminkalenders besteht die Möglichkeit dem Patienten eine Terminfolge per E-Mail zu übermitteln. Dies geschieht auf Basis der bei den Zusatzdaten eingetragenen E-Mail-Adresse des Patienten. Termine selbst werden nur mit einem Kürzel des Patienten eingegeben. Beispiel: Der Patient Max Mustermann (Patienten-Nr.: 35) wird übertragen als Max [35] M. , d.h. es wird nur der erste Buchstabe des Nachnamens übertragen und der Vorname übertragen.

D. Datenschutzrechtliche Bewertung

13 In datenschutzrechtlicher Hinsicht sind die zwischenzeitlich am IT-Produkt erfolgten Änderungen am Verfahren in technischer Hinsicht insgesamt positiv zu bewerten, da integrierten Schnittstellen auf Basis von technischen Neuerungen und auf gesetzlichen Grundlagen erfolgten. Besonders die Anonymisierungsfunktion von Datenbanken für Supportzwecke, nach deren Durchlauf die Daten mit Personenbezug nicht mehr zuordenbar sind.

In rechtlicher Hinsicht hat es im Zeitraum seit der letzten Rezertifizierung zwar Änderungen gesetzlicher Vorschriften gegeben (insbesondere des LDSG Schleswig-Holstein). Hier ist insbesondere der § 6 Abs. 4 LDSG 2012 von Bedeutung1. Neben der Umsetzung der alten Fassung, bei der Protokolldaten nur für einen begrenzten Zeitraum gespeichert werden durften, können Benutzer auch der Forderung des Schleswig-Holsteinischen LDSG nachkommen und die Protokolldaten einer bestimmten Person (der Hersteller spricht hier von Bezugsobjekten) löschen, sobald deren Daten gelöscht wurden. Grundsätzlich können Änderungen an Daten in Protokollen angesehen werden. Das Produkt sieht hierfür eine Übersicht der Patienten vor, für die es Protokolleinträge gibt und sich der Benutzer nun im Einzelnen ansehen kann. Wird ein Patient gelöscht, müssen auch die dazugehörigen Protokolle gelöscht werden. Hierzu wählt der Benutzer den Patienen aus, der nur noch einen Protokolleintrag besitzt und löscht dann unwiderruflich die Protokolldaten. Anschließend ist der Patient in der Liste der Protokolldaten nicht mehr sichtbar. Der Hersteller hat diesen Vorgang in die Dokumentation aufgenommen.

E. Zusammenfassung

14 Zusammenfassend kann dem Produkt Elefant-Profi in der Version 13.02. nach wie vor eine adäquate Umsetzung der Belange des Datenschutzes bescheinigt werden. Es bestehen aus technischer und rechtlicher Sicht keinerlei Bedenken gegen eine Rezertifizierung des Verfahrens.

1 § 6 Abs. 4 LDSG SH: "Werden personenbezogene Daten ausschließlich automatisiert gespeichert, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Die Protokolldaten müssen zusammen mit den gespeicherten personenbezogenen Daten sichtbar gemacht werden können und für den gleichen Zeitraum aufbewahrt werden."

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

Kellinghusen, den _____ Flensburg, den _____

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für IT-Produkte (technisch)

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für IT-Produkte (rechtlich)