

Kurzgutachten zur Erteilung eines Datenschutz- Gütesiegels für Galileo 1.5

_____ im Auftrag der NoemaLife GmbH

_____ datenschutz cert GmbH
13. September 2012
Version 1.2

Inhaltsverzeichnis

1.	Gegenstand der Prüfung	4
2.	Prüfzeitraum und -verfahren	5
3.	Antragstellerin	5
4.	Sachverständige	5
5.	Zweck und Einsatzbereich des Produkts	6
6.	Datenfluss und Schnittstellen des Produktes	6
7.	Bewertung der Änderungen	6
7.1	Änderungen am Produkt	7
7.2	Änderungen in der Einsatzumgebung	10
7.3	Änderungen der rechtlichen Anforderungen	11
7.4	Umsetzung der Vorgaben der OH KIS	11
8.	Zusammenfassung	13

Historie

Version	Datum	Geänderte Kapitel	Änderungsgrund	Bearbeiter
0.1	22.11.2011	Alle	Ersterstellung für Galileo Version 1.2	Dr. Irene Karper; Ralf von Rahden
1.0	09.03.2012	Alle	Finalisierung für Galileo Version 1.2	Dr. Irene Karper; Ralf von Rahden
1.1	10.09.2012	Alle	Überarbeitung für Galileo Version 1.5	Dr. Irene Karper; Ralf von Rahden
1.2	13.09.2012	Alle	Editorielle Überarbeitung	Dr. Irene Karper; Ralf von Rahden

1. Gegenstand der Prüfung

Mit diesem Kurzgutachten werden die Ergebnisse der Auditierung des IT-Produktes „Galileo“ in der Version 1.5 gemäß der Datenschutzauditverordnung Schleswig-Holstein (DSAVO) zusammengefasst, mit der Noema Life GmbH die Prüfstelle datenschutz cert GmbH beauftragt hat. Grundlage der erneuten Prüfung ist der Anforderungskatalog des ULD in der Version 1.2.

Mit Abschluss dieser Auditierung und erfolgreicher Zertifizierung durch das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein erhielt Galileo erneut das Gütesiegel und zeichnet sich damit durch vorbildlichen und nachhaltigen Datenschutz aus.

Galileo wird als klinisches Datenmanagement eingesetzt, integriert medizinische IT-Systeme im Krankenhaus und unterstützt den Workflow am klinischen Arbeitsplatz. Das IT-Produkt wurde erstmals am 30.05.2006 erfolgreich gemäß DSAVO unter dem damaligen Namen „e-health@.solutions“ zertifiziert. Nach der Umbenennung erhielt das Produkt Galileo zuletzt in der Version 1.0 am 19.11.2008 das Gütesiegel des ULD.

Die NoemaLife GmbH hat die Änderungen der Version 1.5 gegenüber der Version 1.0 hat der Hersteller auf der Grundlage einer Selbsterklärung, sowie von Change-Logs und Release Notes dargestellt.

Folgende funktionale Änderungen wurden für die erneute Auditierung als relevant angesehen:

- Überarbeitete Zugriffsrechte,
- Einführung des Datenbankobjektes „Casefile“ als Gruppierung entlang von Falltypen,
- OpenOffice-Integration für die Arztbriefschreibung,
- Report-Plugin zur Auswertung der Protokolldaten,
- Web Start Client,
- Privacy Configuration Module,
- Extended Signature Interface.
- Die Funktionalität des Master Patient Index (MPI) ist nicht mehr Bestandteil von Galileo.

Darüber hinaus gibt es zwei weitere, gegenüber der Produkt-Version 1.0 neue, allerdings optional lizenzierbare Module: „Impersonation“ und „IHE-compliant XDS.b Document Repository“. Diese Module sind nicht Bestandteil der Standardauslieferung von Galileo 1.5 und sind in der Grundeinstellung deaktiviert. Diese Module sind nicht Auditgegenstand und werden daher im Rahmen dieses Gutachtens nur für das Gesamtverständnis unter Kapitel 7.1.8 erörtert.

Folgende Änderungen in der Einsatzumgebung von Galileo 1.5 wurden für die erneute Auditierung als relevant angesehen:

- Umstieg auf Oracle 10g und 11g R2
- Umstieg auf Windows 2008 Server

- Wechsel von TomCat 5.5.11 auf JBoss AS, in der vom Foundation Projekt empfohlenen Version – aktuell: JBoss AS 7
- Unterstützung von Windows Vista und Windows 7; Windows XP und Windows 2000 werden nicht weiter unterstützt
- Aktuelle Browserunterstützung: IE 8 und IE 9, Firefox ab Version 9+
- Umstieg auf Java 1.6 (Server) und 1.7 (für den Client) jeweils in der aktuellen Version.

Für die Auditierung ebenfalls relevant ist die im Jahre 2011 erstmals veröffentlichte „Orientierungshilfe Krankenhausinformationssysteme“ (nachfolgend als OH-KIS bezeichnet) der Unterarbeitsgruppe Krankenhausinformationssysteme der Arbeitskreise Gesundheit und Soziales sowie Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder¹. Die OH KIS bietet zahlreiche Auslegungshilfen für den Datenschutz in Krankenhausinformationssystemen (KIS). Da das IT-Produkt Galileo 1.5 Galileo als klinisches Datenmanagementsystem zur Unterstützung eines genuinen KIS eingesetzt wird, ist es als Bestandteil des KIS bzw. dessen Subsystem zu betrachten. Die Auditierung wurde insofern auf die Prüfung der Vorgaben der OH KIS erweitert.

2. Prüfzeitraum und -verfahren

Die Begutachtung von Galileo 1.5 erstreckte sich auf den Zeitraum vom 30.05.2012 -08.09.2012 und beinhaltet eine konzeptionelle Analyse der von der NoemaLife GmbH zur Verfügung gestellten Unterlagen sowie die Durchführung von Plausibilitäts- und Funktionstests.

3. Antragstellerin

Antragstellerin dieses Gutachtens ist die

NoemaLife GmbH
Alt-Moabit 96
10559 Berlin

als Hersteller des Produkts Galileo. Ansprechpartner ist Herr Arno Helmchen.

4. Sachverständige

Sachverständige Prüfstelle ist die

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen.

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Dr. Irene Karper (Recht). Ansprechpartner für diese Begutachtung sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik).

¹ Z.B. Abrufbar unter http://www.datenschutz.hessen.de/download.php?download_ID=229 (Stand 09/2012).

5. Zweck und Einsatzbereich des Produkts

Galileo wird für klinisches Datenmanagement eingesetzt, integriert medizinische IT-Systeme im Krankenhaus und unterstützt den Workflow am klinischen Arbeitsplatz. Galileo 1.5 kann von Krankenhäusern in öffentlich-rechtlicher Trägerschaft genutzt werden und ist daher grundsätzlich gemäß DSAVO Schleswig-Holstein auditierbar.

6. Datenfluss und Schnittstellen des Produktes

Datenfluss und Schnittstellen des Produktes sind unverändert und werden in der nachfolgenden Übersicht dargestellt.

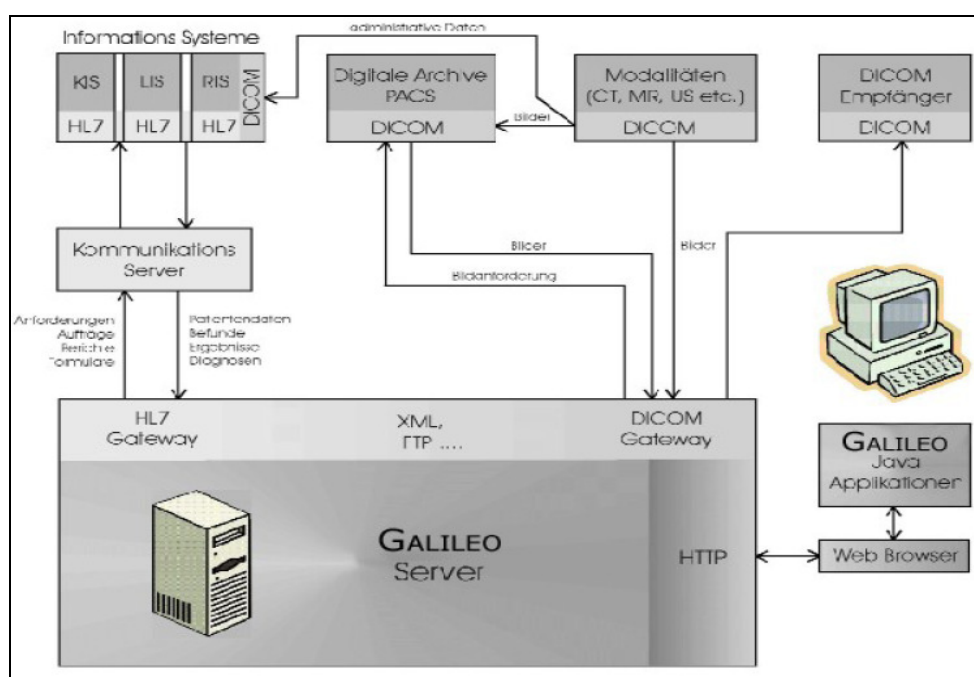


Abb. 1: Schnittstellen und Datenfluss

7. Bewertung der Änderungen

Galileo in der Version 1.5 ist eine Weiterentwicklung des Produkts Galileo 1.0 für klinisches Datenmanagement. Hervorzuheben ist bereits an dieser Stelle, dass die oben genannten Änderungen des Produktes und der Einsatzumgebung zum einen dem Fortschritt der Technik Rechnung tragen, zum anderen die Anforderungen der Orientierungshilfe für Krankenhaus Informationssysteme (OH KIS) weitestgehend umsetzen.

Die Gutachter empfehlen auf der Grundlage der Prüfung der angezeigten Änderungen die erneute Zertifizierung von Galileo 1.5.

Aufgrund der Tatsache, dass das Produkt rezertifiziert werden soll, wird im Folgenden zu den Fragen Stellung genommen,

--- inwieweit das geringfügig veränderte Produkt weiterhin dem Stand der Technik entspricht,

- inwieweit die Einsatzumgebung noch auf einem aktuellen Sicherheits-Stand ist,
- inwieweit die an das Produkt zu stellenden rechtlichen Anforderungen unverändert geblieben sind.

Zudem wird darauf eingegangen, wie Galileo in der Version 1.5 die Vorgaben der OH KIS umsetzt bzw. im Sinne des Datenschutzes fördert.

Im Übrigen wird auf die Ausführungen der Vorauditierungen, insbesondere aus dem Jahre 2008 verwiesen.

7.1 Änderungen am Produkt

7.1.1 Überarbeitete Zugriffsrechte

Die neue Zugriffsrechtestruktur und deren Einstellungsmöglichkeiten sind in der Produktdokumentation detailliert erläutert:

Unterschieden wird zunächst grundsätzlich zwischen Subjekten und Objekten. Es werden seit Galileo 1.4 die Zugriffsrechte von Subjekten auf Objekte festgelegt, wobei das Objekt anhand des Objekttyps und der Objektinstanz charakterisiert wird. Hierbei wird auf ein Rollenmodell verzichtet, da die Rolle eines Subjektes je nach Objekt variieren kann.

So gibt es etwa für einen Patienten (Objekttyp „Patient“, Objektinstanz „Patient A“) für das Subjekt (Arzt X) die Freigabe als „Patient_document_author“, bzw. (Arzt Y) als „Patient_document_filler“, jeweils mit unterschiedlichen Zugriffsrechten auf das Objekt Patient_document für Patient A.

Ferner werden für Objekte ein Security Level (mögliche Werte sind: „Canceled“, „Draft“, „Finalized“) und ein Confidentiality Level festgelegt (mögliche Werte „private“ oder „none“=public). So ist auch hierüber eine Zugriffsfreigabe steuerbar, etwa dass Dokumente mit Security-level „Draft“ nur vom Autor selbst oder von bestimmten Gruppen (etwa Pflegepersonal) nicht geöffnet oder bearbeitet werden kann.

Aus technischer Sicht wird der Freigabeprozess für den Zugriff auf ein Objekt von Decision Managern realisiert. Diese erhalten von sog. Votern eine Ja/Nein-Entscheidung. Je nach implementierter Entscheidungsstrategie (z.B. „alle Voter müssen mit Ja antworten“, oder „mindestens ein Voter muss mit Ja antworten“) treffen die Decision Manager ihre Entscheidung. In der Standard-Auslieferung sind der Global Decision Manager und der Primary Decision Manager implementiert. Optionale können vom Administrator hinzugefügt werden. Die Decision Manager sind hierarchisch strukturiert.

Objekte werden in einer Baumstruktur organisiert. So wird zum Beispiel unter dem Objekt „Patient“ u.a. das Objekt „Visite“ und unter dem Objekt „Visite“ u.a. das Objekt „Visiten-Dokumentation“ angeordnet. Diese Struktur wird ebenfalls für Freigaben genutzt.

Fazit: Die neue Struktur der Zugriffsrechte-Vergabe ist noch detaillierter und erlaubt eine noch feinere Einstellung als zuvor. Auf diese Weise wird der Datenschutz technisch auf vorbildliche Weise unterstützt.

7.1.2 Einführung des Datenbankobjektes „Casefile“

Die Fallakte („Casefile“) ist ein neuer Grouper, welcher medizinische Daten entlang ihrer Fallzugehörigkeit sortiert und anzeigt. Die Fallakte ist als Objekt in Galileo verfügbar, der Zugriff auf die enthaltenen Daten bedarf der entsprechenden Rechte.

Die Einführung hat keine Auswirkungen auf die Zugriffsrechte, sondern dient lediglich der übersichtlicheren Darstellung. Gibt es zu einem Patienten mehrere Fallakten, so befinden sich diese in der Objektstruktur alle unter demselben Objekt „Patient“.

Fazit: Aus sicherheitstechnischer Sicht stellt der neue Grouper keine Veränderung dar.

7.1.3 OpenOffice-Integration für die Arztbriefschreibung

Das OpenOffice Plugin stellt die gleiche Schnittstelle dar, wie sie bereits in Galileo 1.0 für MS Word existiert hat. Es werden die Versionen 3.2 und 3.3 von OpenOffice unterstützt, empfohlen wird die aktuelle portable Version.

Fazit: Die OpenOffice-Integration zusätzlich zur Microsoft Word-Integration stellt keine sicherheitsrelevante Änderung dar. Die Version 3.2 ist für die portable Variante die zurzeit aktuelle Version.

7.1.4 Überarbeitetes Report-Plugin

Das in der Version 1.4 von Galileo eingeführte Report Plugin ist in der Version 1.5 überarbeitet worden.

Zunächst gibt es zwei Reiter, einen für die Anzeige der Notfall-Logins und einen für die Anzeige der normalen Logins. Die Anzeige der Notfall-Logins enthält keine Spalte zur Anzeige der Begründungen für den Notfall-Login. Zur Überprüfung der Begründung im Zweifelsfall muss der Datenschutzbeauftragte des Anwenders zusammen mit dem Administrator auf der Admin-Oberfläche eine gezielte Abfrage stellen. Auf diese Weise wird ein Vier-Augen-Prinzip etabliert.

Die GUI des Report-Plugins bietet der Funktion „Security Officers“ eine Filter- und Sortier-Funktion, die es ihm ermöglichen, Logfiles gezielt auszuwerten. Hierzu werden in einem bestimmten Umfang vordefinierte Filter (User Action, IP, User, Ward) zur Verfügung gestellt. Es lassen sich für das Report-Plugin weitere Filterkriterien implementieren.

Fazit: Das Report-Plugin ermöglicht eine zielgerichtete Auswertung der Protokolle. Auf diese Weise kann z.B. der Datenschutzbeauftragte des Anwenders optimal in seinen Prüfprozessen unterstützt werden. Die Auswertung der Begründung der Notfall-Zugriffe ist zudem über ein Vier-Augen-Prinzip abgesichert. Aus Sicht der Gutachter wird somit der Datenschutz vorbildlich unterstützt.

7.1.5 Web Start Client

Die Client-Application wurde umgestellt von Applet auf WebStart. Auf diese Weise wird die Abhängigkeit zur Kompatibilität von Browser Plugins reduziert.

Fazit: Die Umstellung hat keine sicherheitsrelevanten Auswirkungen. Dadurch, dass weniger Kompatibilitätsprobleme mit Browsern zu erwarten sind, ist die Umstellung zu begrüßen.

7.1.6 Privacy Configuration Module

Der Privacy-Mode für einen Vertraulichkeitsstatus mit einer entsprechenden Beschränkung der Sichtbarkeit von ausgewählten Datenfeldern lässt sich nun komfortabel mit Hilfe einer GUI administrieren. Ein direkter Zugriff auf die Datenbank ist damit nicht mehr nötig.

Fazit: Es liegt keine funktionelle Änderung vor. Lediglich die Administration des Privacy-Modes ist komfortabler gestaltet, wodurch Fehler optimal vermieden werden können, da diese durch die übersichtliche Darstellung leichter entdeckt werden können. Auf diese Weise wird auch die Einhaltung der Datenschutzanforderungen unterstützt.

7.1.7 Extended Signature Interface

Die bereits bestehende Signaturfunktion für Briefe ist erweitert worden. Es lassen sich nun auch bereits gespeicherte Briefe noch nachträglich signieren.

Fazit: Dies hat jedoch keine Auswirkungen auf das Ergebnis der Auditierung, da das Produkt nicht den Anforderungen des Signaturrechts entsprechen muss.

7.1.8 Optionale Module außerhalb des Auditgegenstands

Impersonation Mode: Bevollmächtigung;

Mit dem Impersonation-Mode, welches auf dem deutschen Markt derzeit nicht zur Verfügung steht, kann ein Benutzer seine persönlichen Zugriffsrechte auf Bevollmächtigte übertragen. Der Bevollmächtigte erhält dann mit seinen eigenen Login-Daten denselben Zugriff auf die Daten, wie der Benutzer, der die Bevollmächtigung erteilt hat. Der Impersonation Mode ist als Plugin konzipiert und, sofern installiert, per default deaktiviert. Wird dieser vom Administrator in den Grundeinstellungen aktiviert, so erscheint für den Benutzer von Galileo neben dem Login-Button ein Impersonate-Button. Trägt man sein Benutzernamen und sein Passwort ein und drückt den Impersonate-Button statt des Login-Buttons, so kann man denjenigen Benutzer auswählen, der einem eine Generalvollmacht für den Zugriff auf seine Daten übertragen hat.

Der Benutzer wird im englischen Handbuch darauf hingewiesen, dass die Berechtigung nur im Rahmen der Behandlungskette eingerichtet werden darf, also dass das Patientengeheimnis gewahrt bleiben muss. Da dieses Plugin nicht für den deutschen Markt zur Verfügung steht, ist es im deutschen Handbuch auch nicht dokumentiert.

Fazit: Da der Impersonation Mode optional als Lizenz hinzugenommen werden kann und nicht von der Grundausstattung von Galileo 1.5 umfasst ist, hat dies jedoch keine Auswirkungen auf das Auditergebnis.

IHE-compliant XDS.b Document Repository

Galileo bietet jetzt zudem einen optionalen, separaten Speicher für Dokumente, wie durch das IHE XDS.b Profil beschrieben. Es ist standardmäßig nicht aktiviert, sondern als optionales Plugin konzipiert und gehört daher ebenfalls nicht zum Auditgegenstand.

Die Funktion beruht auf der Access-Rechte-Konfiguration. Der Benutzer muss zuvor in die besonderen Funktionen eingeführt und zudem gesondert vertraglich verpflichtet werden. Die Konformität zum Datenschutz und zu einschlägigen Rechtsvorschriften müssen im Einzelfall vorab vom Anwender dieser Sonderfunktion geprüft werden.

Fazit: Da das XDS.b-Plugin nur optional ist, hat dies keine Auswirkungen auf das Auditergebnis.

7.2 Änderungen in der Einsatzumgebung

Im Rahmen des Übergangs von Galileo 1.0 zu Galileo 1.5 werden in der Einsatzumgebung neuere Versionen der benötigten Software wie folgt unterstützt:

- Umstieg auf Oracle 10g und 11 R2
- Umstieg auf Windows 2008 Server
- Unterstützung von Windows Vista und Windows 7
- Wechsel von TomCat 5.5.11 auf JBoss AS 6.1_final
- Aktuelle Browserunterstützung: IE 8 und IE 9, Firefox ab Version 9
- Umstieg auf Java 1.6 in der aktuellen Version.

Mit Oracle 10g und 11g R2 werden die zwei neuesten Versionen verwendet, wodurch eine Unterstützung über den Zeitraum des angestrebten Gütesiegels hinaus gewährleistet ist.

Dies gilt auch für die Betriebssysteme. Mit dem Umstieg auf Windows 2008 Server und Windows Vista und Windows 7 ist eine langfristige Unterstützung gewährleistet. Windows 2000 und Windows XP werden nicht weiter unterstützt.

Die Unterstützung von IE 8 und IE 9, Firefox ab Version 9 ermöglicht dem Benutzer die Nutzung aktueller Browser. Dies verbessert zusätzlich die Sicherheit.

Mit Java 1.6 und der Empfehlung des Herstellers, die aktuelle Version einzusetzen, werden die neuesten Versionen von Java unterstützt. Client-seitig wird empfohlen die aktuellste Version von Java 1.7 zu verwenden. Die Empfehlung ist ausreichend aktuell.

Sollten Funktionsstörungen auftreten, empfiehlt der Hersteller eine andere (niedrigere) Version zu benutzen. Dies ist Aufgabe des jeweiligen Systemadministrators, der sich bezüglich auftretenden Sicherheitslücken stets auf dem Laufenden halten muss.

Der Applikationsserver Apache TomCat ist durch den JBoss AS in der Version 6.1_final mit allen sicherheitsrelevanten patches abgelöst worden. NoemaLife liefert den JBoss AS nicht mit aus. Es liegt in der Verantwortung des Anwenders,

den JBoss AS sicher zu konfigurieren. Das Sicherheitsniveau hat sich durch den Umstieg von TomCat auf JBoss nicht wesentlich verändert.

Der TomCat App-Server wird nun nur noch zur Administration von JBoss AS und des LauncherAdminTomcat mit den zugehörigen Diensten, wie z.B. HL7-Dienst, genutzt.

Fazit:

Der Umstieg auf die jeweils aktuelleren Versionen von Software in der Einsatzumgebung verbessert die Sicherheit und gewährleistet einen längeren Support für die genutzten Ressourcen.

7.3 Änderungen der rechtlichen Anforderungen

Für die Auditierung waren erneut die Vorgaben der Datenschutzauditverordnung Schleswig-Holstein (DSAVO), des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG S-H)², der Datenschutzverordnung (DSVO)³, das Bundesdatenschutzgesetz (BDSG)⁴ sowie bereichsspezifische Bestimmungen des Gesundheitswesens anzuwenden. Etwa besteht eine Pflicht zur Aufbewahrung von Patientendaten gemäß § 10 der Musterberufsordnung (MBO)⁵ bzw. gemäß der gleichlautenden Berufsordnung für Ärzte des Landes Schleswig-Holstein. Für Röntgenbilder gelten zudem Aufbewahrungsfristen gemäß § 28 der Röntgenverordnung (RöntgenVO)⁶. Im Vordergrund steht dabei allerdings die Wahrung des Patientendatenschutzes. Er wird durch § 203 Strafgesetzbuch (StGB)⁷ und § 9 MBO dargelegt und geschützt.

Die genannten Gesetze haben in der Zwischenzeit keine für das Produkt Galileo relevanten Veränderungen erfahren. In Schleswig-Holstein gibt es ferner noch immer kein Krankenhausgesetz mit Regelungen zur Datenverarbeitung.

Fazit: Die oben beschriebenen Veränderungen an dem Produkt haben auf die bisherige rechtliche Bewertung keine Auswirkungen. Insgesamt ergeben sich demnach keine Veränderungen im Hinblick auf die rechtlich einschlägigen Rahmenbedingungen für das Produkt Galileo und kein Bedarf an einer Änderung des seinerzeit zugrunde gelegten Anforderungsprofils.

7.4 Umsetzung der Vorgaben der OH KIS

Für Galileo 1.5 wurden zudem – wie bereits erörtert - die Vorgaben der „Orientierungshilfe Krankenhausinformationssysteme“ (OH-KIS) der Unterarbeitsgruppe Krankenhausinformationssysteme der Arbeitskreise Gesundheit und Soziales sowie Technik der Konferenz der

² Landesdatenschutzgesetz - LDSG - Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen v. 27.01.2012, GVBl. Schl.-H. 1/2012, S. 78 ff. u. 89 ff.

³ Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten v. 09. 1 2008 , GVOBl Schl.-H. 2008, S. 841ff.

⁴ Bundesdatenschutzgesetz in der Fassung der Bekanntmachung v. 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes v. 14.08.2009 (BGBl. I S. 2814).

⁵ MBO-Ä 1997 in der Fassung der Beschlüsse des 114. Deutschen Ärztetages 2011 in Kiel.

⁶ Röntgenverordnung in der Fassung der Bekanntmachung v. 30.04.2003 (BGBl. I S. 604).

⁷ Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 4 des Gesetzes v. 23.06. 2011 (BGBl. I S. 1266)

Datenschutzbeauftragten des Bundes und der Länder⁸ betrachtet. Die OH KIS enthält fakultative und obligatorische Anforderungen an Hersteller und Betreiber von KIS.

Für Galileo in der Version 1.5 wurden im Rahmen dieses Audits die Herstellerseitigen Vorgaben der OH KIS betrachtet. Die Anforderungen der OH-KIS T 4.6 und 4.7 (Übersicht der vergebenen Berechtigungen), T 4.9 und T 7.7 (Revisionssicherheit der Protokolle), T 7.8 und T 7.17 (Vollständigkeit der Protokolle) und T 7.21 (Exportfunktion von Protokollen zu Analyse Zwecken) werden von Galileo in der Version 1.5 jedoch noch nicht vollständig erfüllt. Es wird noch keine Übersicht der vergebenen Berechtigungen angeboten. Zudem werden die Protokolldaten im Audittrail, insbesondere zeitlich beschränkte erweiterte Zugriffsberechtigungen, derzeit noch nicht revisionssicher gespeichert. Es werden auch nicht alle in der OH KIS geforderten Daten protokolliert. So werden bspw. Suchanfragen oder Zugriffsverweigerungen aufgrund fehlender Berechtigungen nicht protokolliert. Außerdem lassen sich die Protokolle derzeit noch nicht in einem gängigen Format (wie z.B. CSV) zur weiteren Analyse exportieren.

Fazit: Im Ergebnis kann allerdings festgestellt werden, dass Galileo in der Version 1.5 nahezu alle Anforderungen an die „Orientierungshilfe Krankenhausinformationssysteme“ angemessen umsetzt.

Hinsichtlich der derzeit noch offenen Aspekte ist zu berücksichtigen, dass Galileo 1.5 nachhaltig auf die Umsetzung des Datenschutzes ausgerichtet ist und an vielen Stellen über die gesetzlichen Anforderungen in vorbildlicher Weise hinausgeht. Die Auditoren sprechen daher die Empfehlung aus, diese oben genannten Aspekte bis zur nächsten Re-Zertifizierung umzusetzen. Der Hersteller stellt im Übrigen eine Umsetzung dieser Anforderungen für die nächste Version von Galileo bereits in Aussicht.

⁸ Z.B. Abrufbar unter http://www.datenschutz.hessen.de/download.php?download_ID=229 (Stand 09/2012).

8. Zusammenfassung

Das Produkt Galileo in der Version 1.5 erfüllt weiterhin die Anforderungen an den Datenschutz und die Datensicherheit in besonderer Weise, da die verwendeten technischen Lösungen innovativ die Umsetzung der gesetzlichen Vorgaben ermöglichen. Insbesondere das verbesserte Rechte-Konzept und das neue Report-Plugin stellen eine deutliche Verbesserung gegenüber der Vorversion dar. Darüber hinaus wird die OH KIS nahezu vollständig umgesetzt. Gegen eine Re-Zertifizierung bestehen keine Bedenken.

Bremen, 13. September 2012

Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Ralf von Rahden
datenschutz cert GmbH