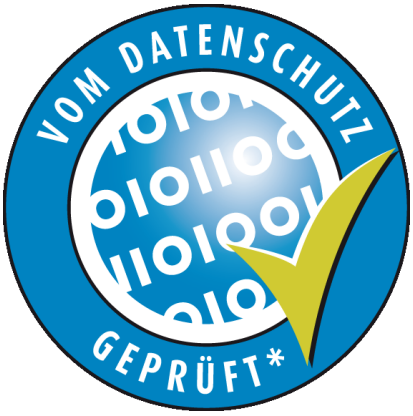

Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

E-Mail-Dienst SafeMail der KVSH

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datum : 02.11.2015
Aktenz. : 16.01/15.002
Telefon : 0431 988 1200
Fax : 0431 988 1223
E-Mail : mail@datenschutzzentrum.de

Inhaltsverzeichnis

1	**Gegenstand des Datenschutzaudits**	**4**
2	**Feststellungen zu den Elementen des Datenschutz-Managementsystems**	**5**
2.1	Aufbau- und Ablauforganisation	5
2.2	Dokumentation des IT-Einsatzes	6
2.3	Sicherheitskonzept	6
2.4	Sicherheitskonzeption auf Infrastrukturebene	7
2.5	Sicherheitskonzeption auf Systemebene	7
2.6	Sicherheitskonzeption auf Anwendungsebene	8
2.7	Sicherstellung und Kontrolle des ordnungsgemäßen Betriebs	9
3	**Datenschutzrechtliche Bewertung**	**10**
3.1	Prüfungsverlauf	10
3.2	Rechtliche Anforderungen	10
3.3	Umsetzung der Regelungen des § 5 Abs. 1 LDSG Abs. 1	12
3.4	Zusammenfassende Bewertung	13

1 Gegenstand des Datenschutzaudits

Das Unabhängige Landeszentrum für Datenschutz (ULD) hat im Jahr 2012 die **Konzeption und Umsetzung** des „**eKVSH E-Mail-Dienstes**“ der Kassenärztlichen Vereinigung Schleswig-Holstein (KVSH) in einem Datenschutzbehördenaudit gemäß § 43 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG) überprüft und bewertet. Im Jahr 2015 wurde der E-Mail-Dienst, der mittlerweile den Namen „**SafeMail**“ trägt, im Rahmen einer Re-Auditierung erneut überprüft.

Der E-Mail-Dienst „SafeMail“ ermöglicht es den am Dienst teilnehmenden Leistungserbringern (insbesondere Arztpraxen, Labore und Krankenhäuser), innerhalb eines geschlossenen Systems elektronische Nachrichten und Dokumente sicher zu versenden. Die Daten werden hierbei sowohl auf Inhaltsebene als auch auf Transportebene durch eine Ende-zu-Ende Verschlüsselung nach aktuellem Stand der Technik gegen Verlust der Vertraulichkeit und Integrität gesichert.

Der Gegenstand des Audit umfasst das Konzept und die Umsetzung des Datenschutz- und Informationssicherheits-Managementsystems für den E-Mail-Dienst „SafeMail“. Überprüft wurden im Rahmen der Reauditierung zum einen Veränderungen am Auditgegenstand, zum anderen erfolgte eine stichprobenartige Überprüfung der Umsetzung des Datenschutz- und Informationssicherheits-Managementsystems.

Vom Audit ausdrücklich nicht erfasst ist die netzwerktechnische Anbindung der Arztpraxen über das geschlossene Netzwerk „KV SafeNet“. Ebenso nicht erfasst sind die erläuternden Darstellungen der KVSH zur Nutzung von SafeMail und die korrekte Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen bei der Nutzung des E-Mail-Dienstes „SafeMail“ innerhalb der Arztpraxen.

2 Feststellungen zu den Elementen des Datenschutz-Managementsystems

2.1 Aufbau- und Ablauforganisation

Die kassenärztliche Vereinigung Schleswig-Holstein (KVSH) ist eine Körperschaft öffentlichen Rechts. Rechtsstellung, Aufgaben, Befugnisse und weitere Regelungen unter anderen zu den Rechten und Pflichten der Mitglieder sind in der Satzung der kassenärztlichen Vereinigung Schleswig-Holstein festgelegt.

Der Vorstand der KVSH trägt die Gesamtverantwortung für den Datenschutz und die Datensicherheit bei der Verarbeitung personenbezogener Daten.

Als behördlicher Datenschutzbeauftragter gemäß § 10 LDSG ist Herr Tom Brümmer bestellt. Er verfügt über die erforderliche Sachkenntnis. Seine anderen dienstlichen Aufgaben stehen in keinem Konflikt mit seiner Tätigkeit als behördlicher Datenschutzbeauftragter. Herr Brümmer ist zentraler Ansprechpartner zur Umsetzung der Betroffenenrechte gemäß § 27ff. LDSG.

Als IT-Sicherheitsbeauftragter der KVSH ist Herr Udo Karlins benannt. Die Aufgaben des IT-Sicherheitsbeauftragten sind in einer IT-Sicherheitsleitlinie festgelegt, die 2014 aktualisiert und im November 2014 (erneut) in der Version 1.0.1 durch den Vorstand verabschiedet wurde. Herr Karlins ist für die Erstellung und Fortschreibung der Sicherheitskonzepte und das Aufrechterhalten des Sicherheitsniveaus verantwortlich. Er ist Mitglied eines IT-Sicherheitsteams und koordiniert die Datenschutz- und Datensicherheitstätigkeiten des Teams. Gemäß IT-Sicherheitsleitlinie ist Herr Karlins frühzeitig bereits in der Planungsphase in alle IT-Projekte einzubinden.

Im Berichtszeitraum 2012-2015 wurden von dem IT-Sicherheitsbeauftragten und dem Datenschutzbeauftragten zahlreiche Fortbildungen (u.a. Personenzertifizierungen) wahrgenommen.

Das IT-Sicherheitsteam setzt sich aus dem behördlichen Datenschutzbeauftragten, dem IT-Sicherheitsbeauftragten und dem IT-Bereichsleiter zusammen. Das IT-Sicherheitsteam unterstützt die Fachbereiche der KVSH bei Fragen der Risikoanalyse- und -bewertung sowie bei der Auswahl angemessener und wirksamer Sicherheitsmaßnahmen.

Der IT-Sicherheitsbeauftragte und der Datenschutzbeauftragte führen anlassbezogene Kontrollen durch. Die Ergebnisse der Kontrollen werden dem IT-Sicherheitsteam und den zuständigen fachlich Verantwortlichen vorgelegt. Der IT-Sicherheitsbeauftrage und der Datenschutzbeauftragte wirken beratend und unterstützend an der Behebung erkannter Mängel mit. Die Mängelbearbeitung wird schriftlich dokumentiert. Das ULD hat die Bearbeitung einzelner Mängel stichprobenartig überprüft.

Der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte führen regelmäßige Kontrollen durch. Der IT-Sicherheitsbeauftragte dokumentiert seine Kontrollen in einem Jahresbe-

richt zur IT-Sicherheit, der dem Vorstand vorgelegt wird. Der Bericht enthält neben den Ergebnissen der Kontrollen auch mit dem Vorstand abgestimmte Kennzahlen zur IT-Sicherheit, eine Beschreibung der IT-Sicherheitsvorfälle sowie eine regelmäßig fortgeschriebene Maßnahmenplanung.

Das ULD hat die Jahresberichte zur IT-Sicherheit stichprobenartig geprüft.

Die allgemeinen organisatorischen Maßnahmen zu Datenschutz und Datensicherheit erfüllen die Anforderungen des § 5 Abs 1. LDSG i.V.m § 3 Abs. 2 Punkt 5 DSVO.

2.2 Dokumentation des IT-Einsatzes

Die KVSH pflegt die gemäß DSVO geforderten Nachweise einer ordnungsgemäßen Datenverarbeitung in einem automatisierten Verfahren. Das Verfahren bietet einen strukturierten Zugriff auf alle für den Betrieb, die IT-Sicherheit und den Datenschutz notwendigen Dokumente und Nachweise.

Der behördliche Datenschutzbeauftragte hat für den E-Mail-Dienst ein Verfahrensverzeichnis erstellt. Das Verzeichnis enthält die in § 7 LDSG vorgeschriebenen Pflichtangaben.

Die Dokumentation wird tool-basiert gepflegt und regelmäßig auf Aktualität und Vollständigkeit geprüft. Ein Auszug der Dokumentation wurde stichprobenartig auf Aktualität überprüft.

Die KVSH pflegt eine Liste der für die Diensterbringung genutzten IT-Systeme. Die Liste enthält unter anderem eine eindeutige Bezeichnung und den Standort der IT-Systeme. Die Anforderungen des § 3 Abs. 2 Punkt 2 DSVO sind erfüllt.

Die Installations- und Konfigurationsdokumentation der Systeme und verwendeten Programme wurde vom ULD stichprobenartig gesichtet. Sie folgt den Vorgaben des Sicherheitskonzepts. Die Anforderungen des § 3 Abs. 2 Punkt 3 DSVO sind erfüllt.

Die physikalischen und logischen Verbindungen der informationstechnischen Geräte sind in Netzwerkplänen dokumentiert. Die Anforderungen des § 3 Abs. 2 Punkt 4 DSVO sind erfüllt.

Die KVSH erbringt den E-Mail-Dienst ausschließlich durch eigenes Personal und selbst betriebene informationstechnische Geräte. Zum Zwecke der Wartung und Beratung wird die KVSH durch externe Auftraggeber unterstützt. Die hierfür notwendigen Verträge gemäß § 17 LDSG sind in die Dokumentation des IT-Einsatzes mit aufgenommen. Die Anforderungen des § 3 Abs. 2 Punkt 8 der DSVO sind erfüllt.

Die Dokumentation ist für sachkundige Personen in angemessener Zeit nachvollziehbar. Die Übereinstimmung der Dokumentation mit der konkreten Datenverarbeitung vor Ort wurde vom ULD stichprobenartig überprüft.

2.3 Sicherheitskonzept

Die KVSH hat für den E-Mail-Dienst ein IT-Sicherheitskonzept erstellt. Das Sicherheitskonzept fasst die einzelnen Dokumente und Nachweise zusammen und gibt einen Überblick über das Verfahren.

Die Auswahl und Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen orientieren sich an der IT-Grundschutz-Vorgehensweise und den Maßnahmenkatalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Einzelne Bestandteile des Sicherheitskonzepts werden in den folgenden Abschnitten dieses Berichts detaillierter dargestellt.

Die in den Konzepten durchgeführte Risikobetrachtung und Maßnahmenauswahl entspricht den Vorgaben des § 4 Abs. 1 bis 3 DSVO.

2.4 Sicherheitskonzeption auf Infrastrukturebene

Die KVSH betreibt personenbezogene Datenverarbeitung an mehreren Betriebsstätten in Bad Segeberg. Die für die Bereitstellung des E-Mail-Dienstes genutzten Räumlichkeiten wurden durch das ULD im Rahmen einer Vor-Ort-Kontrolle geprüft. Im Berichtszeitraum (2012-2015) gab es bauliche Veränderungen im Bereich des Serverraumes, die zu einer Verbesserung des Zutrittsschutzes geführt haben, da Bereiche der Arbeitsvorbereitung nicht mehr Bestandteil des Serverraumes sind und das dort tätige Personal den Serverraum nicht mehr betreten muss.

Die Räume sind klimatisiert und mit einer ausreichend dimensionierten Stromversorgung ausgestattet.

Sämtliche Serversysteme und zentralen Netzwerkkomponenten sind mit einer unterbrechungsfreien Stromversorgung abgesichert, die im Bedarfsfall durch einen Diesel-Generator unterstützt wird. Es erfolgen regelmäßige Tests der Notstromanlage.

Das ULD hat die korrekte Umsetzung der Maßnahmen zur Raum- und Gebäudesicherheit stichprobenartig vor Ort überprüft.

2.5 Sicherheitskonzeption auf Systemebene

Die für die Erbringung des E-Mail-Dienstes verwendeten IT-Systeme umfassen:

- x86-Server zur Virtualisierung auf Basis von VMWare ESXi,
- virtualisierte Serversysteme mit den Betriebssystemen Linux und Microsoft Windows Server und
- zentrale Speichersysteme und
- Einrichtungen zur Datenübertragung sowie aktive Netzwerkkomponenten zur Verkehrslenkung und Netzsegmentierung (Firewalls, Router, Switches).

Die KVSH hält zusätzlich zu den für die Diensterbringung notwendigen Systemen eine virtualisierte Testumgebung bereit. Diese wird für Einzel- und Integrationstests unter anderem bei Aktualisierungen der Betriebssysteme und Anwendungssoftware im Rahmen der Test- und Freigabeverfahren verwendet.

Die auf Systemebene anfallenden Protokolldaten zur Authentifizierung und den Aufruf administrativer Funktionen werden datensparsam und nur zum Zweck der Aufrechterhaltung ei-

nes sicheren und datenschutzkonformen Betrieb der Systeme genutzt.

Eine Protokollierung zu anderen Zwecken, insbesondere denen der automatisierten Verhaltens- und Leistungskontrolle, wird ausgeschlossen. Eine personenbezogene Auswertung der Protokolle darf nur durch dazu berechtigte Personen erfolgen. Die berechtigten Personen sind schriftlich festgelegt.

Die Protokollierung und Kontrolle administrativer Tätigkeiten ist geeignet, die Anforderungen des § 3 Abs. 2 Punkt 6 DSVO i.V.m. § 6 Abs. 2 LDSG zu erfüllen.

2.6 Sicherheitskonzeption auf Anwendungsebene

Der E-Mail-Dienst wird durch die KVSH nur im ebenfalls von der KVSH betriebenen, geschlossenen Netzwerk („KV SafeNet“ genannt) angeboten.

Die für die Mailweiterleitung und –speicherung verwendete Software ist so konfiguriert, dass E-Mails ausschließlich an innerhalb des E-Mail-Dienstes bekannte Postfächer anderer Arztpraxen zugestellt wird. Ein Zustellen von E-Mails an Postfächer in anderen Systemen der KVSH oder Systeme im Internet ist sowohl auf Netzwerkebene als auch auf Softwareebene ausgeschlossen.

Die Software ist weiterhin so konfiguriert, dass ausschließlich verschlüsselte E-Mails und E-Mail-Anhänge akzeptiert werden. Hierzu sind in der Software Filterregeln hinterlegt, die nur gemäß S/MIME-Standard verschlüsselte E-Mails zulassen. Unverschlüsselte E-Mails werden nicht akzeptiert. Entsprechende Konfigurationseinstellungen wurden stichprobenartig überprüft.

Die Verschlüsselung umfasst hierbei den Nachrichteninhalt und mögliche Anhänge. Eine Verschlüsselung des Betreffs der E-Mails findet nicht statt. Die Arztpraxen werden hierauf bei der Beantragung der E-Mailpostfächer hingewiesen. Die Verwendung personenbezogener Daten wie Namen, Vornamen, Patientennummern etc. im Betreff soll seitens der Arztpraxen unterbleiben.

Die in den Postfächern abgelegten, verschlüsselten E-Mails sowie die Protokolldaten werden in einem verschlüsselten Bereich der Dateiablage gespeichert. Hiermit ist sichergestellt, dass Daten zum Absender und Empfänger der E-Mailnachrichten sowie die Betreffzeilen der E-Mails nur verschlüsselt abgelegt werden.

Zur Vergabe und zum Entzug der für die Verschlüsselung verwendeten Schlüssel und Zertifikate betreibt die KVSH eine Software-Lösung, die eine so genannte Certification Authority bereitstellt. Im Rahmen einer geplanten Softwareumstellung wurde die Software zur Erzeugung der Zertifikate erneuert.

Die von der KVSH eingesetzte Software wird weiterhin auf mehreren Servern betrieben, um eine logische Trennung der Registrierung, Zertifizierung und Bereitstellung der Zertifikate zu ermöglichen. Der Zugriff auf die Systeme ist nur einzelnen, explizit berechtigten Mitarbeitern der KVSH möglich. Die Prozesse zur Erstellung von Zertifikaten sind schriftlich festgehalten. Die Durchführung der Prozesse wird schriftlich dokumentiert und die korrekte Dokumentation wird regelmäßig geprüft.

Die mit dieser Software und Hardware erstellten Zertifikate und Schlüssel werden nur für das Sicherstellen der Vertraulichkeit und Integrität der über den E-Mail-Dienst versendeten Nachrichten und Dokumente genutzt. Eine Nutzung der Schüssel und Zertifikate im Sinne einer Signatur gemäß Signaturgesetz findet nicht statt.

Die Verfahren und die Dokumentation der Systeme zur Verwaltung des Schlüsselmaterials erfüllen die Vorgaben des § 4 Abs. 4 DSVO.

2.7 Sicherstellung und Kontrolle des ordnungsgemäßen Betriebs

Administrative Änderungen an den für die Erbringung des E-Mail-Dienstes beteiligten Systemen sind nur einzelnen, explizit berechtigten Mitarbeiterinnen und Mitarbeitern möglich.

Die KVSH hat für die Durchführung der administrativen Tätigkeiten an den vom Auditgegenstand erfassten Systemen konkrete technische und organisatorische Vorgaben in Form einzelner, detaillierter Arbeitsanweisungen getroffen.

Die Arbeitsanweisungen umfassen insbesondere für die Konfiguration des E-Mail-Dienstes und der Verschlüsselung konkrete Einzelschritte und Prüfmaßnahmen. Jegliche Änderung an der Konfiguration der Systeme ist vorab auf einem Testsystem durchzuführen und zu überprüfen.

Sicherheitsmaßnahmen, insbesondere die zur ausschließlich verschlüsselten Weiterleitung und Speicherung getroffenen Einstellungen der verwendeten Softwarekomponenten, werden regelmäßig durch den IT-Sicherheitsbeauftragten geprüft und wurden im Rahmen der Auditierung stichprobenartig geprüft.

Im Rahmen der Weiterentwicklung des Dienstes während des betrachteten Berichtzeitraums 2012-2015 wurden Serverbetriebssysteme konsolidiert. Die vereinfacht die Administrier- und Wartbarkeit. Durch weitere Aufteilung einzelner technischer Funktionalitäten (z.B. Webservices, Authentisierung, Datenbankmanagement) auf verschiedene (virtualisierte) Server wurden Angriffsmöglichkeiten und Verwundbarkeiten auf den Frontsystemen, die von außen erreichbar sind, reduziert. Eine Überwachung der Linux-Betriebssysteme auf das Einspielen erforderlicher Patches erfolgt automatisiert und meldet den Bedarf, Patches manuell einzuspielen. Die dazu erforderlichen Prozesse sind dokumentiert. Die Durchführung der Patchvorgänge wird automatisiert in Logsystemen festgehalten.

Die durch die KVSH getroffenen Maßnahmen zur Dokumentation von Änderungen an informationstechnischen Geräten, Programmen und Verfahren erfüllen die Anforderungen des § 3 Abs. 2 Punkt 6 der DSVO.

Änderungen werden zunächst auf Testsystemen durchgeführt. Die Durchführung der Tests wird schriftlich dokumentiert. Änderungen werden durch die IT-Bereichsleitung nach Abstimmung mit dem IT-Sicherheitsteam freigegeben. Die Anforderungen des § 5 DSVO sind erfüllt.

3 Datenschutzrechtliche Bewertung

3.1 Prüfungsverlauf

Die Reauditierung des E-Mail-Dienstes „**SafeMail**“ wurde vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) in zwei Phasen durchgeführt.

In der ersten Phase wurde durch das ULD die vorgelegte Dokumentation im Hinblick auf Änderungen am Auditgegenstand im Zeitraum von 2012 bis 2015 sowie auf die Vereinbarkeit mit den datenschutzrechtlichen Vorgaben gemäß Landesdatenschutzgesetz Schleswig-Holstein (LDSG) und der Datenschutzverordnung (DSVO) geprüft.

Nach der Dokumentenprüfung hat das ULD in einem Termin vor Ort die Angemessenheit und Wirksamkeit einer Auswahl der in den vorliegenden Dokumenten dargestellten Sicherheitsmaßnahmen stichprobenartig überprüft. Das ULD hat sich durch diese Prüfungen vergewissert, dass die im Konzept dargestellten Maßnahmen seitens der KVSH angemessen und wirksam umgesetzt werden.

Das Auditverfahren wurde durch die ULD-Mitarbeiter Herrn Harald Zwingelberg und Herrn Dr. Thomas Probst durchgeführt.

3.2 Rechtliche Anforderungen

Die Kassenärztliche Vereinigung Schleswig-Holstein (KVSH) ist eine Körperschaft des öffentlichen Rechts.

Sie nimmt für Schleswig-Holstein die ihr gemäß fünftem Buch des Sozialgesetzbuches (SGB V) übertragenen Aufgaben wahr.

Rechtsstellung, Aufgaben, Befugnisse und weitere Regelungen unter anderen zu den Rechten und Pflichten der Mitglieder sind in der Satzung der Kassenärztlichen Vereinigung Schleswig-Holstein festgelegt.

Die fachliche Aufsicht über die KVSH führt die für die Sozialversicherung zuständige oberste Verwaltungsbehörde des Landes. Zum Zeitpunkt des Auditverfahrens ist dies das Ministerium für Soziales, Gesundheit, Wissenschaft und Gleichstellung.

Die KVSH unterliegt bei der Verarbeitung personenbezogener Daten dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG) und der Datenschutzverordnung (DSVO).

Die automatisierte Verarbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen, die die Datensicherheit bzw. die Ordnungsmäßigkeit der Datenverarbeitung gewährleisten. Ein angemessenes IT-Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgaben sind im Informationssicherheits-Managementsystem der KVSH unter der Kontrolle und Mitwirkung des behördlichen Datenschutzbeauftragten zusammengefasst.

Dabei sind insbesondere folgende Rechtsvorschriften zu beachten:

Landesdatenschutzgesetz (LDSG)

§ 4 Datenvermeidung und Datensparsamkeit

§ 5 Allgemeine Maßnahmen zur Datensicherheit

§ 6 Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

§ 7 Verfahrensverzeichnis, Meldung

§ 8 Gemeinsame Verfahren und Abrufverfahren

§ 17 Verarbeitung personenbezogener Daten im Auftrag, Wartung

Telekommunikationsgesetz (TKG)

§ 88 Fernmeldegeheimnis

Datenschutzverordnung (DSVO)

§ 3 Verfahrensdokumentation

§ 4 Dokumentation der Sicherheitsmaßnahmen

§ 5 Dokumentation des Tests und der Freigabe

Darüber hinaus sind interne Regelungen über die personelle und organisatorische Gestaltung der Datensicherheit zu treffen. Es muss gewährleistet sein, dass die datenschutzrechtlichen Anweisungen auch tatsächlich in konkrete Datensicherungsmaßnahmen umgesetzt werden und ihre Einhaltung durch das Informationssicherheits-Managementsystem kontrolliert wird.

Gemäß § 67 SGB V soll zur „Verbesserung der Qualität und Wirtschaftlichkeit der Versorgung“ die papiergebundene Kommunikation so bald und so umfassend wie möglich durch die „elektronische und maschinell verwertbare Übermittlung von Befunden, Diagnosen, Therapieempfehlungen und Behandlungsberichten“ ersetzt werden. Weiterhin ist festgehalten dass die „Krankenkassen und Leistungserbringer sowie ihre Verbände … den Übergang zur elektronischen Kommunikation … finanziell unterstützen“ sollen. Die KVSH bietet den E-Mail-Dienst im Rahmen dieser Aufgabenzuweisung an.

Gemäß § 203 StGB macht sich strafbar, „wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis“ offenbart, das ihm als Arzt anvertraut worden oder sonst bekanntgeworden ist. Die Offenbarung von Patientendaten gegenüber unbefugten Dritten wird durch die durch den E-Mail-Dienst erzwungene Verschlüsselung effektiv unterbunden.

Die KVSH stellt mit dem E-Mail-Dienst **SafeMail** einen Dienst bereit, der sowohl unter die Regelungen des Telekommunikationsgesetzes als auch des Telemediengesetzes fällt. Der

Dienst wird jedoch nur einer geschlossenen Gruppe und nicht der Öffentlichkeit angeboten, so dass Meldepflichten und Maßnahmen aus dem Bereich der öffentlichen Sicherheit nicht einschlägig sind. Die KVSH muss das Fernmeldegeheimnis gemäß § 88 TKG wahren. Die Mitarbeiterinnen und Mitarbeiter der KVSH wurden auf diesen Sachverhalt hingewiesen. Die Systeme des E-Mail-Dienstes stellen eine datensparsame und sichere Verarbeitung der Inhaltsdaten und der näheren Umstände der Telekommunikation sicher.

Im Rahmen von § 67 SGB V unterstützt die KVSH Teilnehmer mit einem Geldbetrag, der sich auch nach dem Aufkommen der mit dem Dienst **SafeMail** versandten E-Mails richtet. Dafür werden sowohl die Zahl der versandten als auch die Zahl der empfangenen E-Mails herangezogen, da sowohl Sender als auch Empfänger gefördert werden sollen: Im Bereich der Teilnehmer gibt es „Vielsender“ (z. B. Labore, Radiologische Praxen), während einzelne Empfänger nur vergleichsweise wenige E-Mails empfangen, aber gleichermaßen eine entsprechende Infrastruktur bereithalten müssen und daher gefördert werden sollen.

Die Anzahl der versandten und empfangenen E-Mails wird teilnehmerbezogen erfasst, um Testnachrichten (E-Mails an sich selbst etc.) bereinigt und ein entsprechender Auszahlungsbetrag, der in der Höhe begrenzt ist, ermittelt und quartalsweise ausgezahlt.

Anhand dieser Erfassung können keine Inhalte der Kommunikation (Inhalte der E-Mails) nachvollzogen werden; insbesondere werden dabei keine Patientendaten erfasst. Allerdings könnte aufgrund der Absender- und Empfängerkennung das Kommunikationsverhalten einzelner Teilnehmer beobachtet werden. Daher werden entsprechende Aufzeichnungen nach der Abrechnung anonymisiert, indem die Teilnehmernummern gelöscht werden. Lediglich eine Fachgruppenbezeichnung (z.B. HNO, Augenarzt, Hausarzt etc.) verbleibt. Die anonymisierten Aufzeichnungen werden für die Kapazitäts- und Wartungsplanung (z. B. zur Bestimmung des optimalen Zeitpunktes für eine Dienstunterbrechung zu Wartungszwecken) benötigt.

3.3 Umsetzung der Regelungen des § 5 Abs. 1 LDSG Abs. 1

Zur Umsetzung der Gewährleistungsziele des § 5 Abs. 1 LDSG wurden u.a. folgende Maßnahmen getroffen:

Verfügbarkeit:

Die Verarbeitung der Daten im Verfahren SafeMail erfolgt mit redundanten virtuellen und physikalischen Servern in einem Cluster. Es erfolgen regelmäßige Datensicherungen, mit der virtuelle Systeme in kurzem Zeitrahmen wiederhergestellt werden können. Die Räumlichkeiten sind gegen physikalische Gefahren (u.a. Brand, unbefugte Zutritte, Stromausfälle) besonders gesichert.

Vertraulichkeit:

Die mit dem Verfahren SafeMail versandeten E-Mails werden mit einem Publik-Private-Key-Verfahren verschlüsselt. Die Schlüssel werden so erzeugt, dass die KVSH keine Kenntnis von den privaten Schlüsseln der Teilnehmer hat, aber ihre Authentizität und Zuordnung zu Teilnehmern sicherstellen kann. Ein Versand ist nur innerhalb des Mailverbundes SafeMail

möglich. Der Versand unverschlüsselter E-Mails wird unterbunden.

Integrität:

Der Zugriff auf Verfahrenskomponenten und -server ist nur besonders berechtigten Administratoren möglich. Ein inhaltlicher Zugriff auf Daten der E-Mails ist wegen der Verschlüsselung nicht möglich.

Transparenz:

Das Verfahren ist hinsichtlich der Konzeption, der verwendeten Programme und Systeme einschließlich ihrer Konfiguration mit einem Dokumentationstool nachvollziehbar dokumentiert. Einzelne Übertragungsvorgänge von verschlüsselten E-Mails werden im Rahmen einer Protokollierung überwacht, sind aber wegen der Verschlüsselung inhaltlich nicht nachvollziehbar.

Nichtverkettbarkeit:

Patientendaten werden nur innerhalb der verschlüsselten E-Mails, nicht aber im Rahmen der unverschlüsselten Betreffzeilen verarbeitet. Für die KVSH sind daher im Rahmen des SafeMail-Versandes keinerlei Patientendaten sichtbar.

Einzelne versandte E-Mails können über die Absender- und Empfängerkennungen der Teilnehmer miteinander verkettet werden. Dies ist im Rahmen der Gewährung von Zuschüssen an die Teilnehmer je nach Anzahl versandter und empfangender E-Mails erforderlich. Die dabei anfallenden Abrechnungsdaten für die Teilnehmer werden gesondert aufbewahrt und fristgerecht gelöscht.

Intervenierbarkeit:

Die Ausübung der Rechte der betroffenen Patienten sind durch die beteiligten Kommunikationspartner (Teilnehmer) zu gewährleisten, da nur diese Zugriffe auf die patientenidentifizierenden Informationen haben. Die Ausübung der Rechte der Teilnehmer wird durch den Datenschutzbeauftragten der KVSH unterstützt.

3.4 Zusammenfassende Bewertung

Im Auditverfahren „**SafeMail**“ wurde festgestellt, dass die KVSH weiterhin über eine rechts- und normenkonforme Konzeption für einen E-Mail-Dienst für Arztpraxen verfügt.

Die Umsetzung der Konzeption umfasst angemessene und wirksame technische und organisatorische Sicherheits- und Datenschutzmaßnahmen nach aktuellem Stand der Technik.

Das Datenschutz- und Sicherheitsmanagement orientiert sich an internationalen Standards und insbesondere an den Vorgaben des Standards 100-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI). Auf Ebene der technischen und organisatorischen Maßnahmen folgt das Informationssicherheits-Managementsystem den Vorgaben der IT-Grundschutz-Vorgehensweise gemäß Standard 100-2 des BSI und zieht Sicherheitsmaßnahme aus den Grundschutz-Katalogen für die Sicherheitskonzeption heran.

Darüber hinaus wurden bei der Durchführung des Audits folgende Aspekte festgestellt, die

im Sinne einer **datenschutzkonformen und –fördernden Gestaltung von Technik und Organisation** besonders hervorzuheben sind:

1. Datenschutzbeauftragter und IT-Sicherheitsbeauftragter arbeiten in und mit einem Managementsystem für den Datenschutz und die Informationssicherheit, welches durch regelmäßige und anlassbezogene Kontrollen ein hohes Maß an Datenschutz sicherstellt. Definierte Prozesse zur Bearbeitung von Datenschutz- und Sicherheitsvorfällen sowie eine funktionierende Einbindung in IT-Projekte bereits in der Planungsphase sind geeignet, das hohe Niveau zu halten.
2. Die Sicherheitsprozesse sind unter Berücksichtigung eines national anerkannten Sicherheitsstandards gestaltet. Das Datenschutzmanagement orientiert sich eng an den Vorgaben zur Ordnungsmäßigkeit der Datenverarbeitung der Datenschutzverordnung (DSVO).
3. Die technischen und organisatorischen Abläufe des Datenschutz- und Informationssicherheits-Managementsystems sind vollständig und nachvollziehbar beschrieben. Das verwendete automatisierte Verfahren zur Dokumentation ermöglicht eine strukturierte Ablage der Dokumentation und Nachweise.
4. Der E-Mail-Dienst stellt durch technische Maßnahmen sicher, dass nur verschlüsselte Nachrichten und Anhänge versendet werden können. Der E-Mailverkehr der Arztpraxen wird mit Verschlüsselungsverfahren nach aktuellem Stand der Technik gesichert.

Die Prüfung hat ergeben, dass das Datenschutz- und Informationssicherheits-Managementsystem sowie die technischen und organisatorische Umsetzung keinen Anlass zu datenschutzrechtlichen Beanstandungen geben. Der Auditgegenstand wird ordnungsgemäß betrieben. Die Verarbeitung personenbezogener Daten ist rechtmäßig.

Kiel, 2. November 2015

(Auditor Recht: Harald Zwingelberg) (Auditor Technik: Dr. Thomas Probst)