Deutsche Röntgengesellschaft

@GIT Arbeitsgemeinschaft Informationstechnologie

gmds

Datenschutzrechtliches Gutachten

Datenschutzrechtliche Bewertung der DICOM-E-MAIL-Standardempfehlung der AG Informationstechnologie der Deutschen Röntgengesellschaft e.V.

Autor: Dr. Bernd Schütze
Leiter der Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V.

Inhaltsübersicht

Kapitel 1 Einleitung 3

Kapitel 2 Darstellung des Begutachtungsgegenstandes 5

Kapitel 3 Rechtliche Rahmenbedingungen 6

Kapitel 4 Rechtliche Grundlage der Verarbeitung 11

Kapitel 5 Schutz der informationellen Selbstbestimmung des Betroffenen 13

Kapitel 6 Hinweise für die Weiterentwicklung 18

Kapitel 7 Fazit 19

Kapitel 8 Conclusion 21

Kapitel 9 Glossar 22

Übersicht Begutachtung 23

Inhaltsverzeichnis

Kapitel 1 Einleitung 3

Kapitel 2 Darstellung des Begutachtungsgegenstandes 5

2.1 Beschreibung des Begutachtungsgegenstandes 5

2.2 Ausgangsbedingungen 5

2.3 Abgrenzung 5

2.4 Vorgelegte Dokumente 5

Kapitel 3 Rechtliche Rahmenbedingungen 6

3.1 Personenbezogene Daten 6

3.2 Besondere Arten der personenbezogenen Daten 6

3.3 Sozialdaten 7

3.4 Berufliche Schweigepflicht 7

3.5 Datenverarbeitung im Auftrag 9

3.6 Zusammenfassung Kapitel 3 10

Kapitel 4 Rechtliche Grundlage der Verarbeitung 11

4.1 Rechtsvorschrift 11

4.2 Einwilligung 11

Kapitel 5 Schutz der informationellen Selbstbestimmung des Betroffenen 13

5.1 Authentifizierung des Absenders 13

5.2 Authentizität und Integrität der Daten 14

5.3 Verbindlichkeit 15

5.4 Vertraulichkeit der Daten 15

5.4.1 Verschlüsselung der Daten 15

5.4.2 Verschlüsselung der Kommunikation 16

5.4.3 Schutz von Sender und Empfänger 16

5.5 Anmerkungen zum „Web of Trust“ 17

Kapitel 6 Hinweise für die Weiterentwicklung 18

Kapitel 7 Fazit 19

Kapitel 8 Conclusion 21

Kapitel 9 Glossar 22

Übersicht Begutachtung 23

Kapitel 1 Einleitung

Teleradiogische Anwendungen, die in den derzeit auf dem Markt befindlichen PACS-Lösungen integriert sind, erlauben in der Regel keinen direkten herstellerübergreifenden und sicheren Datentransfer, wie dies beispielsweise mit den meisten im Internet verwendeten Protokollen (z.B. E-Mail, FTP, Telnet) möglich ist. Diese (proprietären) Anwendungen zeigten schon früh den Nutzen teleradiologischer Anwendungen in der Radiologie auf, zugleich wurden aber die Grenzen der Teleradiologie ohne einen herstellerübergreifenden Standard aufgezeigt.

Das DICOM-Treffen 2003 in Mainz zeigte, dass im PACS-Umfeld im Schnittstellenbereich der DICOM-Standard (StoreSCU, StoreSCP) verwendet wird. Jedoch wird die Wegstrecke der Datenfernübertragung auf unterschiedliche Weise gelöst, wodurch ein direkter Datenaustausch zwischen den Kommunikationspartner unterbunden wurde[1]. Die Teilnehmer dieses Treffens waren überzeugt, dass ein allgemeingültiger Konsens über die Definition einer geeigneten Schnittstelle mit dem Ziel von herstellerunabhängigen interoperablen Teleradiologie-Anwendungen notwendig und möglich ist1. Die Arbeitsgemeinschaft Informationstechnologie (@GIT) der Deutschen Röntgengesellschaft (DRG) gründete daher 2003 die Initiative zur Standardisierung der Teleradiologie.

In mehreren Sitzungen der Initiative wurden die grundlegenden Probleme diskutiert und analysiert. Die verschiedenen Konfigurationen der Firewall-Lösungen in den unterschiedlichen stationären und ambulanten Einrichtungen gestatteten eine spontane Verbindung lediglich über die E-Mail-Kommunikation. Supplement 54 des DICOM-Standards („Supplement 54: DICOM MIME-Type“) bietet die Möglichkeit, DICOM-Datentypen als MIME-Attachment in eine E-Mail einzubinden[2]. MIME (Multipurpose Internet Mail Extension) beschreibt, wie Dateien als Anhang („Attachement”) an eine E-Mail angehängt und so mittels SMTP (Simple Mail Transfer Protocol) an Kommunikationspartner übermittelt werden können. Das Supplement beschreibt hierbei genau, wie die Umsetzung eines DICOM-Datentyps in ein MIME-Attachement zu erfolgen hat, so dass die Teleradiologie-Initiative der @GIT hierauf wie auch auf den entsprechenden RFC (Request for Comments) aufbauen konnte[3].

Zum Schutz der sensiblen Patientendaten entschied sich die Teleradiologie-Initiative für eine Verschlüsselung nach dem Open-PGP-Standard, welche zugleich eine verlustfreie Kompression nach dem zip-Standard ermöglicht. Auch wurde eine Empfehlung zum Einsatz von PGP zur Übermittlung medizinischer Daten mittels E-Mail schon 2001 abgegeben[4]. Der Vorteil der Lösung gegenüber vielen anderen Lösungsszenarien bestand von Anfang an darin, dass der Empfänger ausschließlich ein E-Mail-Programm sowie eine Möglichkeit zur Entschlüsselung benötigt. Da heutzutage jeder medizinisch Tätige eine E-Mail-Lösung einsetzt und Ver- sowie Entschlüsselungssoftware entsprechend dem OpenPGP-Standard für jedes Betriebssystem und nahezu jeden E-Mail-Client existiert, wird somit keine spezielle Software beim Empfänger benötigt: der Austausch von Patientendaten wird dadurch enorm vereinfacht.

---

[1] Mildenberger P, Kämmerer M, Engelmann U, Ruggiero S, Klos G, Runa A, Schröter A, Weisser G,Walz M, Schütze B. (2005) Empfehlungen der @GIT für einen Standard für telemedizinische Anwendungen unter Verwendung von DICOM-E-Mail. Fortschr Röntgenstr 177(5): 697 - 702

[2] DICOM Standard Status [Online] 2015 [zitiert 2015-06-24]; Verfügbar unter http://www.dclunie.com/dicom-status/status.html#FinalSupplementsSince2011

[3] Digital Imaging and Communications in Medicine (DICOM) - Application/dicom MIME Sub-type Registration [Online] 2004 [zitiert 2015-06-24]; Verfügbar unter ftp://ftp.rfc-editor.org/in-notes/rfc3240.txt

[4] Henkel M. (2001) Übermittlung elektronischer Arztdaten. Radiologe (41):M 21–24.

In den vergangenen Jahren zeigte sich immer wieder, wie wichtig der Schutz der Daten vor unbefugtem Zugriff ist. Darauf wurde beim DICOM-E-Mail-Standard von Anfang an Wert gelegt. Dennoch ist es nach 12 Jahren stetiger Weiterentwicklung des DICOM-E-Mail-Standard wichtig, den Standard hinsichtlich der Umsetzung von Datenschutz und Datensicherheit überprüfen zu lassen.

Die Arbeitsgruppe Datenschutz und IT-Sicherheit im Gesundheitswesen (DIG) der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) zeigte durch ihre Kommentierungen[5] und Ausarbeitungen[6] die hierfür notwendige Fach- und Sachkenntnis, sowohl im Bereich der technischen wie auch der rechtlichen Fragen. Daher wurde der Leiter dieser Arbeitsgruppe um eine datenschutzrechtliche Begutachtung des DICOM-E-Mail-Standard gebeten.

[5] Stellungnahmen der AG "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG). [Online] 2015 [zitiert 2015-06-24]; Verfügbar unter http://www.gesundheitsdatenschutz.org/doku.php/gmds-dgi-stellungnahmen

[6] Empfehlungen der AG "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG). [Online] 2015 [zitiert 2015-06-24]; Verfügbar unter http://www.gesundheitsdatenschutz.org/doku.php/gmds-dgi-empfehlungen

Kapitel 2 Darstellung des Begutachtungsgegenstandes

2.1 Beschreibung des Begutachtungsgegenstandes

Der von der @GIT veröffentlichte DICOM-E-Mail-Standard dient dem gesicherten Datenaustausch von Gesundheitsdaten, insbesondere Patientendaten, zwischen an einem Behandlungsprozess beteiligten Personen. Der Datenaustausch erfolgt unter Nutzung des MIME-konformen E-Mail-Verfahrens, die Sicherheit der Gesundheitsdaten wird durch eine entsprechende Verschlüsselung gewährleistet. Neben der Datenübertragung beschreibt der Standard auch grundlegende Funktionalitäten, welche typischerweise ein Verzeichnisdienst anbietet.

Gegenstand dieser Begutachtung sind einerseits die Komponenten des Datenaustausches, dies beinhaltet die Beschreibung der Verschlüsselung sowie die dargestellte Authentifizierung der am Datenaustausch beteiligten Menschen und die Gewährleistung der Konsistenz der Daten durch die im DICOM-E-Mail-Standard beschriebene Erweiterung des Mail-Standards.

Andererseits werden auch in den angesprochenen Verzeichnisdienst-Funktionalitäten personenbezogene Daten der Kommunikationspartner abgebildet, sodass der Schutz dieser Daten ebenfalls Teil dieser Begutachtung ist.

2.2 Ausgangsbedingungen

Die Entwicklung des DICOM-E-Mail-Standard begann am 2. September 2003, die erste Version des Standards wurde 2004 veröffentlicht. Seit diesem Zeitpunkt wird der Standard kontinuierlich weiterentwickelt. Das Gutachten bezieht sich auf die derzeitige Version 1.7.

2.3 Abgrenzung

Es werden nur die im DICOM-E-Mail-Standard beschriebenen Dienste bzw. Funktionalitäten in diesem Gutachten betrachtet. Nicht Gegenstand dieser Begutachtung sind technische und/oder organisatorische Maßnahmen, welche bei Anwendung dieses Standards projektbezogen umzusetzen sind. Jedoch werden an geeigneter Stelle Hinweise auf zu treffende ergänzende Maßnahmen gegeben.

2.4 Vorgelegte Dokumente

Die Dokumentation des DICOM-E-Mail-Standard in Version 1.7.1 vom Juli 2013, verfügbar auf der Homepage http://www.agit.drg.de/de-DE/1228/dicom-e-mail-standardempfehlung.

Kapitel 3 Rechtliche Rahmenbedingungen

3.1 Personenbezogene Daten

Alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“) gelten entsprechend Artikel 2 a) RL 95/46/EG als personenbezogene Daten[7], analog der Vorgabe der Richtlinie erfolgt die Definition in §3 Abs. 1 BDSG[8]. Daten von Firmen, Institutionen und Organisationen (z. B. einer GMBH) fallen damit nicht unter die datenschutzrechtliche Schutzwirkung. Ausgenommen hiervon sind Sachverhalte, bei denen mit den Daten eindeutig eine natürliche Person identifiziert werden kann, wie dies z. B. eine Firma bestehend aus einer Person, wie dies beispielsweise in einer kleineren Arztpraxis vorkommen kann, der Fall ist.

Im DICOM-E-Mail-Standard werden Daten von potentiell drei Personenkreisen erhoben, verarbeitet und genutzt:

1) Der Versender der Nachricht
2) Der Empfänger der Nachricht
3) In der Nachricht befindliche Daten, die als personenbezogene Daten anzusehen sind.

3.2 Besondere Arten der personenbezogenen Daten

Der DICOM-E-Mail-Standard beschreibt die Übertragung medizinischer Daten mittels des Mail-Protokolls. Diese Daten sind i. d. R. einer Person (Patient/Patientin) zugeordnet. Art. 8 Ziff. 1 RL 95/46/EG werden Daten über Gesundheit der besonderen Kategorien personenbezogener Daten zugerechnet, deren Schutzbedarf als besonders hoch anzusehen ist. Die Verarbeitung dieser Daten ist gemäß Art. 8 Ziff. 1 RL 95/46/EG grundsätzlich untersagt, außer

a) es liegt eine Einwilligung der betroffenen Person vor und die nationale Gesetzgebung verbietet die Verwendung der Daten nicht explizit
b) die Verarbeitung ist erforderlich, um dem Arbeitsrecht zu genügen, d. h. es ist eine arbeitsrechtliche Erlaubnisnorm vorhanden
c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten erforderlich und die Person ist aus physischen oder rechtlichen nicht in der Lage, die Einwilligung zu geben
d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation, die keinen Erwerbszweck verfolgt im Rahmen ihrer rechtmäßigen Tätigkeiten und die Verarbeitung bezieht nur auf die Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten

oder

e) die Verarbeitung bezieht sich auf Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich.

[7] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. [Online, zitiert am 2015-06-22]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=de

[8] Bundesdatenschutzgesetz (BDSG): § 3 Weitere Begriffsbestimmungen. [Online, zitiert am 2015-06-22]; Verfügbar unter http://www.gesetze-im-internet.de/bdsg_1990/__3.html

Die Artikel 29 Gruppe veröffentlichte im Februar 2015 ein White Paper[9], nach dem der Begriff „Gesundheitsdaten“ aus Sicht des europäischen Gesetzgebers nicht nur medizinische Daten („medical data“) umfasst, sondern vielmehr medizinische Daten nur als Teilmenge der Gesundheitsdaten („health data“) aufzufassen sind. Dementsprechend ist der Begriff der Gesundheitsdaten sehr weitestgehend zu verstehen. Als Beispiele werden von der Artikel 29 Gruppe genannt:

- Informationen, ob eine Person eine Brille oder Kontaktlinsen trägt.
- Die Mitgliedschaft in einer Vereinigung zur Hilfe von bestimmten Krankheitsgruppen („patient support groups“ in Unterscheidung zu „self-help groups“).

Im deutschen Recht findet sich die Begrifflichkeit der „personenbezogene Daten der besonderen Art“ in §3 Abs. 9 Bundesdatenschutzgesetz (BDSG) wieder.

3.3 Sozialdaten

Die Legaldefinition von Sozialdaten findet sich in §67 Abs. 1 Sozialgesetzbuch X (SGB X). Demnach sind Sozialdaten alle „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in §35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden“. Sozialdaten sind somit ausschließlich personenbezogene oder personenbeziehbare Daten, die von Sozialleistungsträgern erhoben, verarbeitet oder genutzt werden. Damit sind Sozialdaten eine Teilmenge der Gesundheitsdaten.

Die Leistungsträger sind gemäß §35 SGB I zur Wahrung des Sozialgeheimnisses sind entsprechend §12 in Verbindung mit §§18 bis 29 SGB I verpflichtet. Die Verwendung von Sozialdaten ist gemäß §35 Abs. 2 SGB I nur unter den Voraussetzungen der §§67a-78 SGB X (= Zweiter Abschnitt „Datenerhebung, -verarbeitung und -nutzung) zulässig, die datenschutzrechtlichen Bestimmungen entsprechend der der §§78a-85a SGB X sind hierbei zu beachten.

3.4 Berufliche Schweigepflicht

Die Verpflichtung zur Einhaltung einer ärztlichen Schweigepflicht ist sowohl im Strafgesetzbuch (§ 203 StGB) als auch in den Berufsordnungen der Landesärztekammern (§ 9 BO) festgelegt. Allerdings bezieht §203 StGB Abs. 1 Ziff. 1 nicht allein den ärztlichen Beruf in den Kreis der zur Schweigepflicht bestimmten ein, sondern umfasst „Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert“. Demnach gehören u.a. auch folgende medizinische Berufsgruppen zu den unter §203 StGB fallenden Berufszweigen:

- Diätassistentin/ Diätassistent
- Heilpraktikerin / Heilpraktiker
- Podologin/ Podologe
- Altenpfleger
- Hebamme / Entbindungspfleger
- Physiotherapeut
- Ergotherapeut
- Gesundheits- und Kinderkrankenpflegerin/ Gesundheits- und Kinderkrankenpfleger

[9] Artikel-29-Datenschutzgruppe (2015-02-05) White Paper “ANNEX – health data in apps and devices”. [Online, zitiert am 2015-06-14]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

- Gesundheits- und Krankenpflegehelferin/ Gesundheits- und Krankenpflegehelfer
- Gesundheits- und Krankenpflegerin/ Gesundheits- und Krankenpfleger
- Notfallsanitäter.

Der strafrechtlichen Schweigepflicht unterliegen auch die bei dem Schweigepflichtigen berufsmäßig tätigen Gehilfen und die Personen, die zur Vorbereitung auf den Beruf an der entsprechenden Tätigkeit teilnehmen, also z. B. Verwaltungsmitarbeiter im Bereich der Abrechnung der erbrachten Leistungen oder im Bereich des Qualitätsmanagement.

Der geschützte Geheimbereich ist dabei weit zu ziehen: zum geschützten Bereich gehören sowohl die Tatsachen und Umstände, die sich auf den Gesundheitszustand des Patienten selbst beziehen als auch alle Gedanken, Meinungen, Empfindungen, Handlungen, familiären, finanziellen und beruflichen Verhältnisse, an deren Geheimhaltung der Patient oder ein Dritter, auf den sich das Geheimnis bezieht, erkennbar ein Interesse hat[10]. Selbst die Tatsache, dass sich ein Patient überhaupt in ärztlicher Behandlung befindet oder befunden hat, zählt - ebenso wie natürlich der Name des Patienten - zu dem vom Gesetz geschützten Geheimbereich[10].

Im Gegensatz zu datenschutzrechtlichen Vorgaben[11] gilt die aus §203 StGB resultierende Schweigepflicht über den Tod des Patienten hinaus.

Der Tatbestand des §203 StGB setzt voraus, dass einer der in Abs. 1 genannten Geheimnisverpflichteten ein fremdes Geheimnis, welches ihm anvertraut worden ist, unbefugt offenbart. Schutzzweck der Vorschrift ist vorrangig die Geheimsphäre des Einzelnen, daneben auch das Allgemeininteresse an der Verschwiegenheit einzelner Berufsgruppen[12]. Ein Offenbaren im Sinne des §203 StGB ist demnach zunächst jede Mitteilung über die geheim zu haltende Tatsache an einen Dritten[13].

Dem Wortlaut nach würde bereits die Weitergabe der Geheimnisse an das Pflegepersonal oder Sprechstundenhilfe eine Offenbarung bedeuten. Da dies jedoch jeglichen Funktionsablauf in einer Arztpraxis oder einem Krankenhaus zum Erliegen bringen würde, entspricht es herrschender Ansicht, dass beim Einsatz derartige Hilfskräfte kein Offenbaren im Sinne des §203 StGB vorliegt (entsprechend §203 Abs. 3 S. 2 StGB, wonach auch diejenigen zur Verschwiegenheit verpflichtet sind, die den Schweigepflichtigen in Bezug auf dessen berufliche Tätigkeit unterstützen). Ein Offenbaren liegt auch dann nicht vor, wenn der Empfänger des Geheimnisses „zum Kreis der zum Wissen Berufenen" gehört, beispielsweise wenn ein weiterer Arzt (Radiologe, Labormediziner, …) im Behandlungsprozess des Patienten integriert ist.

Werden im Rahmen eines Outsourcings hingegen „externe" Dienstleister mit diesen Aufgaben betraut, so werden die Geheimnisse nicht an interne Mitarbeiter weitergegeben, sondern über die Grenzen von juristischen Personen hinweg ausgetauscht. Insbesondere stellt das BDSG keine Offenbarungsbefugnis dar, da entsprechend §1 Abs. 3 S. 2 BDSG dies ausschließt[14].

Allerdings wird entsprechend §205 Abs. 1 StGB ein Verstoß gegen §203 StGB nur auf Antrag verfolgt, wobei entsprechend §77 Abs. 1 StGB nur

---

[10] Ärztekammer Berlin. (2008) Merkblatt Schweigepflicht. [Online, zitiert am 2015-06-14]; Verfügbar unter http://www.aerztekammer-berlin.de/10arzt/30_Berufsrecht/08_Berufsrechtliches/06_Behandlung_von_Patienten_Pflichten_Empfehlungen/35_Merkblatt_Schweigepflicht.pdf

[11] Dammann U. (2014) §3 Abs. 1 Rn. 17. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlagsgesellschaft. ISBN 978-3-8487-0593-1

[12] Bräutigam P. (2011) §203 StGB und der funktionale Unternehmensbegriff - Ein Silberstreif am Horizont für konzerninternes IT-Outsourcing bei Versicherern. CR: 411-416

[13] Ehrmann, Outsourcing von medizinischen Daten – strafrechtlich betrachtet-, 2008,S. 60

[14] Bundesdatenschutzgesetz (BDSG): § 1 Zweck und Anwendungsbereich des Gesetzes. [Online, zitiert am 2015-06-14]; Verfügbar unter http://www.gesetze-im-internet.de/bdsg_1990/__1.html

- der Verletzte (= der betroffene Patient)
- bzw. im Falle, dass der Antragsberechtigte geschäftsunfähig oder beschränkt geschäftsfähig ist, der gesetzliche Vertreter
- oder - nach dem Tod des Verletzten - der Erbe

zu einem Antrag auf Strafverfolgung berechtigt ist.

3.5 Datenverarbeitung im Auftrag

Unter einer „Datenverarbeitung im Auftrag“ (i. d. R. als Auftragsdatenverarbeitung, in Kurzform ADV, bezeichnet) wird gemäß §11 BDSG die „Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung“ personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers verstanden.

Der Begriff des „Auftragsverarbeiter“ wird in Artikel 2 lit. e der Richtlinie 95/46/EG definiert[15]:

> *"Auftragsverarbeiter" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.*

Entsprechend Art. 6 Abs. 2 der Richtlinie 95/46/EG ist der „für die Verarbeitung Verantwortliche“ für die Einhaltung der datenschutzrechtlichen Vorschriften (Art. 6 Abs.1 der Richtlinie 95/46/EG) verantwortlich. Der Auftragsverarbeiter wird nur im Rahmen der Vorgaben des für die Verarbeitung Verantwortlichen tätig, ist somit nur im Rahmen der Einhaltung der ihm gemachten Vorgaben datenschutzrechtlich verantwortlich. Die Artikel 29 Gruppe erarbeitete 2010 eine Stellungnahme[16] zu diesen Begrifflichkeiten, damit diese europaweit gleich verwendet werden.

Dementsprechend definiert die Richtlinie 95/46/EG in Art. 2 lit. f den Begriff des „Dritten“:

> *"Dritter" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten.*

Die Definition findet sich in §3 Abs. 8 BDSG wieder.

Nach deutschem Recht findet eine Datenübermittlung nur dann statt, wenn Daten einem Dritten zur Verfügung stehen (§3 Abs. 4 Ziff. 3 BDSG). Dies ist im Rahmen einer Auftragsverarbeitung wichtig, da hier bei der Verwendung der Daten durch den Auftragnehmer datenschutzrechtlich keine Übermittlung im Sinne von §3 Abs. 4 Ziff. 3 BDSG stattfindet. Somit bleibt zwar der Auftraggeber datenschutzrechtlich verantwortliche Stelle, da jedoch keine Übermittlung stattfindet, wird für die Verwendung der Daten durch den Auftragnehmer im Auftrag des Auftraggebers keine gesonderte Rechtsvorschrift oder die Einwilligung des Betroffenen benötigt.

[15] RL 95/46/EG, Artikel 2 “Begriffsbestimmungen”. [Online, zitiert am 2015-06-14]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=de

[16] Artikel-29-Gruppe (2010) Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“. [Online, zitiert am 2015-06-14]; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

3.6 Zusammenfassung Kapitel 3

Der DICOM-E-Mail-Standard beschreibt die Übertragung medizinischer Daten, wobei es sich in aller Regel um personenbezogene oder personenbeziehbare Gesundheitsdaten handelt. Diese Daten gehören datenschutzrechtlich zu den Datenkategorien, welche den höchsten Schutzbedarf aufweisen. Eine Teilmenge der Gesundheitsdaten bilden die Sozialdaten, deren Verwendung in Deutschland durch die Gesetzgebung enge Grenzen gesetzt sind.

Personen, die einer ärztlichen Berufsgruppe angehören oder zu den Apothekern gehören bzw. Angehörige eines anderen Heilberufs sind, welcher für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, unterliegen einer besonderen Schweigeverpflichtung entsprechend §203 StGB. Wer ein fremdes Geheimnis offenbart, welches ihm in der Ausübung seines Berufes anvertraut wurde, begeht eine Straftat. D. h. Daten, die dieser Verpflichtung unterliegen, bedürfen neben einer datenschutzrechtlichen Erlaubnisnorm zur Weitergabe zusätzlich einen entsprechenden strafrechtlich befreienden Erlaubnistatbestand, z. B. eine Schweigepflichtentbindung.

Eine Auftragsdatenverarbeitung stellt eine datenschutzrechtliche Erlaubnisnorm dar, nach welcher ein Auftragnehmer Daten ausschließlich entsprechend den Weisungen des Auftragnehmers verwenden darf, jedoch stellt eine Auftragsdatenverarbeitung alleine keine Offenbarungsbefugnis im Sinne des §203 StGB dar.

Kapitel 4 Rechtliche Grundlage der Verarbeitung

Entsprechend §4 Abs. 1 BDSG[17] ist eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Im Rahmen der Betrachtung des DICOM-E-Mail-Standard ist nicht abzuleiten, auf Grund welcher Erlaubnisnorm Daten im Sinne des BDSG erhoben, verarbeitet oder genutzt werden, da der Standard nur allgemein beschreibt, wie Daten mittels des E-Mail-Protokolls sicher transportiert werden. Dennoch muss natürlich an dieser Stelle auf die Begrifflichkeiten der Rechtsvorschrift bzw. der Einwilligung eingegangen werden.

4.1 Rechtsvorschrift

Unter dem Begriff „Rechtsvorschrift" sind „alle materiellen Rechtsnormen mit unmittelbarer Außenwirkung"[18] zu verstehen, d. h. insbesondere zählen alle in Deutschland geltenden Gesetze und Rechtsverordnungen dazu. Weiterhin zählen der normative Teil von Tarifverträgen wie auch Betriebs- und Dienstvereinbarungen dazu, wenn diese eine unmittelbare Außenwirkung aufweisen[19]. Es ist allerdings fraglich, ob Vereinbarungen in Tarifverträgen oder Betriebs- bzw. Dienstvereinbarungen das Schutzniveau des BDSG unterschreiten dürfen.

Hingegen zählen Regelwerke wie Erlasse oder Verwaltungsvorschriften nicht zu den Rechtsnormen im Sinne des §4 Abs. 1 BDSG[18].

4.2 Einwilligung

Die Definition von Einwilligung bzw. welche Bedingungen zu einer datenschutzrechtlich geltenden Einwilligung erfüllt sein müssen, stellt die Artikel-29-Gruppe in Working Paper 187[20] „Definition von Einwilligung" vor.

Eine Einwilligung einer betroffenen Person setzt eine „Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden[20]" voraus. Diese Anforderung findet sich in §4a Abs. 1 Bundesdatenschutzgesetz wieder. Das Bundesdatenschutzgesetz gibt im Gegensatz zur Richtlinie 95/46/EG sogar die Form der Willensbekundung vor: „Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist[21]".

Gemäß Artikel 7 Absatz a) Richtlinie 95/46/EG muss die betroffene Person ihre Einwilligung „ohne jeden Zweifel" gegeben haben. Auch wenn diese Forderung so nicht im deutschen Recht abgebildet wurde, gibt es keinerlei Zweifel daran, dass diese Anforderung auch in Deutschland gilt. Damit diesem Anspruch genügt wird, „darf ein Verfahren zur Einholung und Erteilung der Einwilligung keinen Zweifel an der Einwilligungsabsicht der betroffenen Person lassen[20]".

[17] Bundesdatenschutzgesetz (BDSG): § 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung [Online, zitiert am 2015-06-15]; Verfügbar unter http://www.gesetze-im-internet.de/bdsg_1990/__4.html

[18] Dix P, Sokol B. §4 Abs. 1 3 Rn. 9 in Simitis (Hrsg.) Bundesdatenschutzgesetz. 8. Auflage. Nomos Verlag. ISBN 978-3-8487-0593-1

[19] Vgl. z.B. BAG Urteil vom 20.12.1995 (AZ 7 ABR 8/95) oder BAG Urteil vom 30.08.1995 (AZ 1 ABR 4/95)

[20] Artikel-29-Datenschutzgruppe. (2011) Definition von Einwilligung. [Online, zitiert am 2015-06-15]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

[21] Bundesdatenschutzgesetz: § 4a Einwilligung. [Online, zitiert am 2015-06-15]; Verfügbar unter http://www.gesetze-im-internet.de/bdsg_1990/__4a.html

Indirekt verbunden ist damit auch der Nachweis der Einwilligung: Kann die oder der für die Datenverarbeitung Verantwortliche nicht nachweisen, dass eine Einwilligung vorlag, so muss das Vorhandensein der Einwilligung bezweifelt werden. Dies kann bedeuten, dass die Verarbeitung der Daten der betroffenen Person rechtlich nicht erlaubt war.

Bei Daten, die zu einer „besonderen Kategorie personenbezogener Daten" entsprechend Art. 8 Richtlinie 95/46/EG gehören, verlangt Art. 8 Abs. 2 lit. a zudem eine „ausdrückliche" Einwilligung. Das Bundesdatenschutzgesetz bildet diese Forderung in §4a Abs. 3 ab. Eine implizite Einwilligung (z. B. Opt-out-Lösungen) genügen dieser Anforderung nicht.

Zusammenfassend stellen sich die Erfordernisse an eine datenschutzrechtlich wirksame Einwilligung wie folgt dar:

- Eine Einwilligung durch den Betroffenen muss freiwillig erfolgen.
- Eine Einwilligung bedarf der Schriftform.
- Der Betroffene muss insbesondere auf folgende Punkte hingewiesen werden:
  - Zweck der Speicherung
  - Ggf. die Übermittlung an Dritte, wenn dies dem Verwendungszweck enthalten ist
  - Die Geltungsdauer der Einwilligung muss für den Betroffenen eindeutig ersichtlich sein.
  - Dem Betroffenen muss mitgeteilt werden, dass er immer eine auf die zukünftige Verwendung ausgerichtete Widerrufsmöglichkeit bzgl. der erteilten Einwilligung besitzt. Zugleich muss ihm mitgeteilt werden, dass der Widerruf natürlich nur eine Verarbeitung und Nutzung der Daten nach seinem Widerruf betreffen kann, d. h. dass ein Widerruf nicht in die Vergangenheit wirken kann.
  - Dem Betroffenen muss mitgeteilt werden, dass er immer ein Recht auf Korrektur wie auch auf Löschung seiner Daten besitzt.
  - Auf Nachfrage durch den Betroffenen muss auf eventuelle Folgen der Verweigerung der Einwilligung hingewiesen werden.
  - Soweit nicht offensichtlich muss dem Betroffenen mitgeteilt werden:
    - Wer ist die verantwortliche Stelle?
    - Welche Daten werden erhoben?

Kapitel 5 Schutz der informationellen Selbstbestimmung des Betroffenen

Die mittels des DICOM-E-Mail-Standards übermittelten Daten dienen - direkt oder indirekt (z. B. als Ergebnis von Forschungsvorhaben oder qualitätssichernden Maßnahmen) - der Mit- oder Weiterbehandlung von Menschen. Daher ist es wichtig, dass der Empfänger der Daten einerseits den Sender der Daten einwandfrei authentifizieren kann, andererseits sich sicher sein kann, dass die von ihm verwendeten Daten unverändert bei ihm ankamen. Zugleich muss natürlich gewährleistet sein, dass die Daten während des Transportes nicht von Unbefugten eingesehen werden können.

5.1 Authentifizierung des Absenders

Der DICOM-E-Mail-Standard verlangt in Kapitel 17 verpflichtend, dass alle übermittelten Daten mit einer elektronischen Signatur des Senders versehen werden. Somit kann der Empfänger die Identität des Empfängers eindeutig bestimmen, solange der für die elektronische Signatur verwendete Schlüssel nicht kompromittiert ist.

Zur Erzeugung einer digitalen Unterschrift verweist der DICOM-E-Mail-Standard auf den OpenPGP-Standard sowie die entsprechenden RFCs. OpenPGP[22] erlaubt die Nutzung folgender Algorithmen zur Erzeugung eines für eine elektronischen Signatur erforderlichen Hashwertes:

- MD5
- RIPEMD-160
- SHA-1
- SHA224
- SHA256
- SHA384
- SHA512.

Entsprechend den heutigen Erkenntnissen sind nicht mehr alle Algorithmen geeignet, die Sicherheit einer elektronischen Signatur zur gewährleisten. Beispielsweise ist seit 2004[23] bei MD5 bekannt, das mit einem vergleichsweise geringen Aufwand die Erzeugung unterschiedlicher Nachrichten mit dem gleichen MD5-Hashwert und damit ggfs. die gleiche elektronische Signatur zu erzeugen.

Zur Erzeugung einer elektronischen Signatur erlaubt OpenPGP die Nutzung der folgenden Algorithmen[22]:

- RSA
- DSA.

Der OpenPGP-Standard definiert weiterhin keine Schlüssellänge[22]. Daher ist seitens des DICOM-E-Mail-Standard nicht gewährleistet, dass anhand der auf dem OpenPGP-Standard übermittelten elektronischen Signatur eindeutig der Empfänger der Daten identifiziert werden kann. In Anbetracht der Sensibilität der Daten, die durch Nutzung dieses Standards übertragen werden sollen, muss daher gefordert werden, dass beim jeweiligen Einsatzszenario vertraglich die verbindliche Nutzung eines als sicher geltenden Algorithmus wie auch einer entsprechend als sicher geltenden Schlüssellänge vereinbart werden.

[22] RFC 4880 OpenPGP Message Format. [Online, zitiert am 2015-06-16]; Verfügbar unter http://www.ietf.org/rfc/rfc4880.txt

[23] Wang X, Feng D, Lai X, Yu H. (2004) Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. [Online, zitiert am 2015-06-16]; Verfügbar unter http://eprint.iacr.org/2004/199.pdf

Jährlich veröffentlicht die Bundesnetzagentur einen Algorithmenkatalog[24] bzgl. Signatur- und Verschlüsselungsverfahren sowie zur Generierung von Hashwerten, der auch im Bundesanzeiger publiziert wird, der aktuelle Katalog findet sich unter der Nummer „BAnz AT 30.01.2015 B3“[25]. Das BSI empfiehlt ebenfalls kryptographische Verfahren und Schlüssellängen[26]. Idealerweise greift der DICOM-E-Mailstandard die Empfehlungen seitens BSI bzw. der Bundesnetzagentur auf bzw. referenziert die Empfehlungen und schränkt die verwendbaren Algorithmen und Schlüssellängen entsprechend ein.

5.2 Authentizität und Integrität der Daten

Neben der sicheren Identifikation des Absenders bietet die elektronische Signatur die Gewähr, dass die Daten während des Transportes nicht verändert wurden. Allerdings gilt hier das im Abschnitt 5.2 bzgl. der Auswahl von Algorithmus und Schlüssellänge bei OpenPGP ausgeführte: Der OpenPGP-Standard alleine gewährleistet keine sichere elektronische Signatur.

Laut Kapitel 18.3 können Daten auf mehrere E-Mails verteilt werden. In diesem Fall kann der Empfänger nicht wissen, wie viele E-Mails der Sender verschickte und ob er alle Daten bekommen hat. Somit ist alleine durch das E-Mail-Protokoll nicht die Integrität der Daten zu gewährleisten. Der DICOM-E-Mail-Standard beschreibt für diesen Fall der Aufsplittung der Daten auf mehrere E-Mails zwei optionale Verfahren, die zur Gewährleistung der Beurteilung der Vollständigkeit der erhaltenen Daten genutzt werden können:

a) Eine standardkonforme Erweiterung des E-Mail-Headers (Kapitel 18.4.1), in welcher die Gesamtzahl der versendeten E-Mails sowie die jeweilige Nummer der Mail inklusiver einer eindeutigen ID enthalten ist.
b) Die Nutzung der E-Mail-Empfangsbestätigung (Kapitel 18.4.2).

Entsprechend Kapitel 18.4.2.1 ist die Nutzung der Empfangsbestätigung verpflichtend. Allein durch die Empfangsbestätigung kann der Empfänger jedoch die Vollständigkeit der Daten nicht ersehen, lediglich der Datenversender weiß - sofern die per E-Mail-Protokoll übermittelte Empfangsbestätigung bei ihm ankommt -, ob alle Daten beim Empfänger angekommen sind oder nicht. Der Empfänger kann die Vollständigkeit der Daten nur durch Nutzung der laut Standard optional nutzbaren Erweiterung des E-Mail-Headers beurteilen.

Daher ist eine Gewährleistung der Datenintegrität für den Empfänger nur gegeben, wenn die Nutzung der standardkonformen Erweiterung des E-Mail-Headers im jeweiligen Einsatz gewährleistet ist, d. h. die Optionalität z. B. durch eine vertragliche Regelung zwischen den sendenden Parteien ausgeschlossen wird.

---

[24] Bundesnetzagentur. Auflistung geeigneter Algorithmen und Parameter. [Online, zitiert am 2015-07-27]; Verfügbar unter http://www.bundesnetzagentur.de/cln_1431/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen-node.html

[25] Bundesanzeiger. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen). [Online, zitiert am 2015-07-27]; Verfügbar unter https://www.bundesanzeiger.de/ebanzwww/wexsservlet?page.navid=official_starttoofficial_view_publication&session.sessionid=a7c31d51ee61337b6f9504eeb1128417&fts_search_list.selected=a5a498db9a76afd5&&fts_search_list.destHistoryId=38555&fundstelle=BAnz_AT_30.01.2015_B3

[26] Bundesamt für Sicherheit in der Informationstechnik (BSI). Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1). [Online, zitiert am 2015-07-27]; Verfügbar unter https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30924/BSI-TR-02102_V1_0_pdf.pdf

5.3 Verbindlichkeit

Ebenso, wie der Empfänger eine Sicherheit bzgl. der Identität erlangen muss, ist es für den Datenversender wichtig zu wissen:

a) Alle Daten sind beim Empfänger angekommen.
b) Der Empfänger hat die Daten gesehen.

Wie schon beschrieben ist gemäß Kapitel 18.4.2.1 die Nutzung der Empfangsbestätigung verpflichtend, d. h. für jede Mail, die der Empfänger erhielt, wird eine Empfangsbestätigung an den Sender verschickt, wobei die Empfangsbestätigung die eindeutige Identifikationsnummer der versendeten Mail enthält. So erhält der Sender eine Übersicht, welche Daten nachweislich beim Empfänger angekommen sind und kann ggfs. auf unbestätigte E-Mails mit einem erneuten Versand reagieren. Dies kann bedeuten, dass der Empfänger einzelne E-Mails mehrfach erhält, was aber im Sinne des medizinischen Kontextes, in welchem dieser Standard agiert, zur Gewährleistung der Datensicherheit als zumutbar beurteilt werden muss.

Bei der Beurteilung im jeweiligen Szenario muss unter Beachtung der jeweils eingesetzten Softwarelösung jedoch ggfs. darauf geachtet werden, dass ein automatischer erneuter Versand bei Fehlen einer E-Mail-Bestätigung nach einem Zeitraum „x“ zu einer Denial-of-Service-Attacke genutzt werden kann, z. B. durch aktiver Unterdrückung des Empfangs der Notification-E-Mails des Empfängers.

Der DICOM-E-Mail-Standard gewährleistet somit, dass die E-Mails in der Softwarelösung des Empfängers angekommen sind, d. h. die E-Mails vom Mailserver des Empfängers abgerufen wurden. Der Standard kann jedoch keine Auskunft darüber geben, ob der Empfänger die Daten auch zur Kenntnis genommen hat. Je nach Szenario, in welchem der Standard eingesetzt wird, sind zur Gewährleistung der Sicherheit der Patientenversorgung organisatorische Maßnahmen verpflichten zu vereinbaren, welche hier die notwendige Gewissheit der Kenntnisnahme der Daten gewährleisten.

5.4 Vertraulichkeit der Daten

Die medizinischen Daten eines Menschen gehören zu den Daten mit dem höchsten Schutzbedarf. Daher ist eine ungeschützte Datenübertragung nicht statthaft.

5.4.1 Verschlüsselung der Daten

Entsprechend Kapitel 16 müssen alle Daten entsprechend RFC 4880 mit OpenPGP verschlüsselt werden. Im Kapitel 16 wird zwar ein Hinweis zur Auswahl eines geeigneten Algorithmus sowie einer geeigneten Schlüssellänge in Form eines Links zu einer Technischen Richtlinie (TR-02102) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) angeboten, aber einerseits besteht hier keine Verpflichtung zum Befolgen der Empfehlung der Technischen Richtlinie, andererseits führt der Link beim BSI zu einer Fehlerseite. Der Fehler bzgl. des Links sollte beseitigt werden[27].

OpenPGP gestattet entsprechend RFC 4880 folgende Algorithmen zur Verschlüsselung der Daten[22]:

- RSA
- Elgamal
- IDEA
- TripleDES / 3DES

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Online, zitiert am 2015-06-16]; Verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

- Cast5
- Blowfish
- AES
- Twofish.

Bei einigen Verfahren wird die Schlüssellänge vorgegeben (z. B. Cast5 = 128 Bit Schlüssellänge). Auch hier muss gesagt werden, dass mit den vom OpenPGP-Standard erlaubten Algorithmen und Schlüssellängen eine sichere Verschlüsselung möglich ist, aber nicht zwingend erfolgen muss. Wie schon bzgl. Nutzung der elektronischen Signatur beschrieben ist es aufgrund des Schutzbedarfs der vom DICOM-E-Mail-Standard adressierten Daten erforderlich, dass die zwingende Verwendung als sicher geltender Algorithmen wie auch als sicher geltende Schlüssellängen bei der Übermittlung medizinsicher Daten gewährleistet ist.

5.4.2 Verschlüsselung der Kommunikation

Der Versand von E-Mails erfolgt mittels des SMTP-Protokolls, der Abruf von E-Mails vom Mailserver geschieht unter Nutzung des das POP3- oder des IMAP-Protokolls. Alle drei Protokolle sind textbasierte Protokolle, d. h. mittels eines Telnet-Clients kann eine E-Mail auch „von Hand“ verschickt oder empfangen werden. Dementsprechend wird eine unverschlüsselte Nutzung der Protokolle auch mit dem Versand einer Postkarte verglichen: alles Geschriebene ist von jedem, der die Postkarte in die Hand bekommt, lesbar.

Beim Transfer höchst sensibler Daten, wie es die vom DICOM-E-Mail-Standard adressierten Gesundheitsdaten darstellen, sollten die Protokolle ausschließlich unter Nutzung einer Transportverschlüsselung genutzt werden. Transport Layer Security (TLS) bzw. Secure Sockets Layer (SSL) ergänzen die Protokolle SMTP. POP3 und IMAP um die für eine Verschlüsselung erforderlichen Funktionalitäten. Seit SSL Version 3.0 wird das SSL-Protokoll unter den Namen TLS verwendet. Die SSL-Versionen vor 3.0 weisen diverse Sicherheitslücken auf und sollten daher nicht verwendet werden.

Stand heute (Juni 2015) muss der Einsatz von StartTLS entsprechend RFC 2595[28] in Verbindung mit RFC 4616[29] bei IMAP und POP3 gefordert werden bzw. RFC 3207[30] bei SMTP. Der DICOM-E-Mail-Standard weist im Kapitel 22.1 auf RFC 2995 zwar hin, fordert dessen Einsatz aber nicht. Daher muss auch hier in Anbetracht der Sensibilität der Daten, die durch Nutzung des DICOM-E-Mail-Standard übertragen werden sollen, gefordert werden, dass beim jeweiligen Einsatzszenario vertraglich die verbindliche Nutzung einer entsprechend verschlüsselten E-Mail-Kommunikation vereinbart wird.

5.4.3 Schutz von Sender und Empfänger

Analog zum Brief müssen beim Versand Sender und Empfänger bekannt sein:

1) es muss bekannt sein, wohin die Daten transportiert werden sollen,
2) es muss bekannt sein, wer informiert werden soll, wenn
    a) die Zustellung nicht erfolgen konnte oder
    b) wer bzgl. der erfolgreichen Zustellung informiert werden soll.

[28] RFC 2995 Using TLS with IMAP, POP3 and ACAP. [Online, zitiert am 2015-06-16]; Verfügbar unter https://tools.ietf.org/html/rfc2595
[29] RFC 4616 The PLAIN Simple Authentication and Security Layer (SASL) Mechanism. [Online, zitiert am 2015-06-16]; Verfügbar unter https://tools.ietf.org/html/rfc4616
[30] RFC 3207 SMTP Service Extension for Secure SMTP over Transport Layer Security. [Online, zitiert am 2015-06-16]; Verfügbar unter http://www.ietf.org/rfc/rfc3207.txt

Daher müssen rudimentäre Angaben zu Sender und Empfänger unverschlüsselt übertragen werden. Im Header einer jeden E-Mail finden sich daher entsprechend den Vorgaben stets die folgenden Informationen:

```
Return-Path: <sender@adresse-sender.de>
X-Original-To: empfänger@adresse-empfaenger.de
Delivered-To: mailserver.adresse-empfaenger.de
Received: from mailserver.adresse-sender.de (mailserver.adresse-
     sender.de [IP-Adresse])
     by mailserver.adresse-empfaenger.de (Mailserversoftware) with
     ESMTPS id ID-Nummer
     for < empfänger@adresse-empfaenger.de >; Wed, 24 Jun 2015
     13:13:13 +0200 (CEST)
Received: from sender.client.hardware ([IP-Adresse]);
     by mailserver.adresse-sender.de running Mailserver-Software
     id ID-Nummer; Wed, 24 Jun 2015 13:11:11 +0200
From: <sender@adresse-sender.de>
To: < empfänger@adresse-empfaenger.de>
Subject: Worum geht es in dieser E-Mail eigentlich
Date: Wed, 24 Jun 2015 13:10:40 +0200
Message-ID: <Nachricht-ID-Nummer@adresse-sender.de >
MIME-Version: 1.0
Content-Type: Welche Art NAchricht - Nur Text, HTML-Mail, ...
X-Mailer: Client-Software des Senders
Content-Language: de
```

Die Angaben der E-Mailadresse von Sender und Empfänger findet sich damit immer unverschlüsselt in jeder Mail, hier kann auch der DICOM-E-Mail-Standard die darin enthaltenen personenbezogenen Daten nicht schützen.

Allerdings können sich auch in dem „Betreff"-Teil („subject") einer E-Mail personenbezogene Daten vorhanden sein, der DICOM-E-Mail-Standard enthält hier keine Vorgaben. Da dieser Teil im Header der Mail unverschlüsselt enthalten ist, sind Angaben, die hier enthalten sind ungeschützt.

5.5 Anmerkungen zum „Web of Trust"

Es muss bemerkt werden, dass das sogenannte „Web of Trust" nicht dem Sicherheitsbedarf bei der Übermittlung medizinischer personenbezogener Daten genügt. Vielmehr muss jeder Schlüssel eindeutig nachweisbar einer natürlichen Person zugeordnet werden können (z. B. durch Vorlage Personalausweis oder Postident-Verfahren), wobei diese identifizierte Person für die sichere Aufbewahrung und ordnungsgemäße Verwendung des Schlüssels verantwortlich ist. Dem steht natürlich nicht entgegen, dass auch Organisationsschlüssel verwendet werden können; ein entsprechender Organisationsschlüssel muss jedoch einer für die Organisation im juristischen Sinne vertretungsberechtigten Person zugeordnet werden und bei Wechsel der Person muss zugleich der Schlüssel ausgewechselt werden. (Dies beinhaltet im Sinne von OpenPGP den Rückruf des „alten" Schlüssels.)

Die Vorgaben zu einer entsprechenden Public-Key-Infrastruktur (PKI) sind nicht Bestandteil des DICOM-E-Mail-Standards, jedoch muss darauf hingewiesen werden, dass die Sicherheit des Standards direkt abhängig von der Sicherheit der verwendeten Schlüssel ist. D. h. eine sichere Verwendung des DICOM-E-Mail-Standard ist nur mit einer entsprechenden Organisation inklusive PKI möglich.

Kapitel 6 Hinweise für die Weiterentwicklung

Im Standard sollte festgelegt werden, welche Algorithmen und Schlüssellängen verwendet werden dürfen, desgleichen sollte an die Sicherheit der zur Verschlüsselung genutzten Geheimnisse („Schlüssel“) Mindestanforderungen gestellt werden, dies betrifft sowohl die Generierung wie auch den Umgang/Nutzung und den Rückruf. Im internationalen Umfeld gibt es in verschiedenen Ländern Gesetze, welche einige ggfs. die Güte der Verschlüsselung gesetzlich regeln, evtl. sogar einschränken. Daher sollte überlegt werden, ob im Standard nationale Ergänzungen vorgesehen werden, in welchem diese und ähnliche Elemente, die von einer nationalen Gesetzgebung abhängig sind, national geregelt wird.

Der Mail-Header sollte dahingehend überarbeitet werden, dass er so wenig personenbezogene bzw. personenbeziehbare Daten wie möglich enthält. Insbesondere sollten Vorgaben erstellt werden, wie mit dem „Betreff“/„Subject“-Teil der E-Mail umzugehen ist, d. h. hier sollten explizit Vorgaben im DICOM-E-Mail-Standard erarbeitet werden, dass hier auf keinen Fall patientenbezogene Daten zu finden sind, idealerweise auch keine personenbezogenen Daten von Sender und Empfänger.

Kapitel 7 Fazit

Der DICOM-E-Mail-Standard nutzt zur Übertragung von patientenbezogenen Daten standardkonform das Transportmedium E-Mail. Zum Schutz der Gesundheitsdaten werden diese entsprechend dem OpenPGP Standard verschlüsselt.

Standardbedingt werden alle im Header einer E-Mail übertragenen Daten unverschlüsselt übertragen, dazu gehören insbesondere die E-Mailadresse von Sender und Empfänger wie auch die im „Betreff"-Teil einer E-Mail befindlichen Angaben. Die E-Mailadresse von Sender und Empfänger werden zum Transport einer E-Mail zwingend benötigt, so dass deren Schutz durch Verschlüsselung kaum zu leisten ist. Bzgl. der Angaben im Betreff fehlt im DICOM-E-Mail-Standard jeglicher Hinweis bzgl. des Umgangs mit diesem Feld, insbesondere ist kein Hinweis zu den Risiken vorhanden, die mit der Nutzung des Feldes bei der Eingabe von personenbezogenen oder personenbeziehbaren Daten eingegangen werden. Im Sinne einer datenschutzfreundlichen Lösung wünscht man sich eine Erweiterung des Standards in dem

a) auf die Risiken einer unverschlüsselten Übermittlung von Daten innerhalb des Betreff-Feldes hingewiesen wird sowie
b) Vorgaben für die DICOM-E-Mail-Standardkonforme Nutzung des Betreff-Feldes im Hinsicht auf personenbezogene Daten existieren.

Im DICOM-E-Mail-Standard existieren keinerlei Vorgaben zur Verwendung des Verschlüsselungsalgorithmus und der Schlüssellänge. Der OpenPGP Standard enthält Algorithmen zur Verschlüsselung wie auch zur elektronischen Unterschrift, welche als sicher anzusehen sind. Desgleichen enthält der Standard aber auch Algorithmen, die aus heutiger Sicht als unsicher gelten und deren Nutzung keine Sicherheit der Daten gewährleistet. Bei den derzeit noch als sicher geltenden Algorithmen muss einschränkend bemerkt werden, dass deren Sicherheit auch von der Schlüssellänge abhängig ist. Da weder der DICOM-E-Mail- noch der OpenPGP-Standard hier Vorgaben definieren, ist sowohl eine sichere wie auch eine unsichere Übertragung von Daten mittels des DICOM-E-Mail-Standard möglich - je nach Nutzung.

Weder im DICOM-E-Mail- noch im OpenPGP-Standard finden sich Vorgaben bzgl.

- der Erzeugung des für die OpenPGP-konforme Verschlüsselung notwendigen Schlüsselpaares (privater und geheimer Schlüssel),
- der Aufbewahrung und Nutzung des Schlüsselpaares sowie
- des evtl. notwendigen Rückrufes des Schlüsselpaares.

Auch bei Auswahl von sicheren Algorithmen und einer hinlänglich starken Schlüssellänge ist die Sicherheit der Verschlüsselung maßgeblich davon abhängig davon, wie sicher der für die Verschlüsselung benutzte Schlüssel ist. Bei Gesundheitsdaten, welche zu den mit am höchsten zu schützen geltenden Daten gehören, ist hier zwingend erforderlich, dass

- die Generierung des Schlüsselpaares dergestalt erfolgte, dass nur der Berechtigte den geheimen Schlüssel erhält, d.h. zu keinem Zeitpunkt eine Kopie an Dritte erfolgen konnte
- die Aufbewahrung und Nutzung des privaten Schlüssels so erfolgt, dass nur der Berechtigte Zugriff auf den privaten Schlüssel erhält
- bei Kompromittierung des geheimen Schlüssels ein Rückruf möglich ist und so eine Benutzung durch unbefugte Dritte verhindert wird.

Eine konforme Nutzung des DICOM-E-Mail-Standard alleine gewährleistet somit keine sichere Datenübertragung. Vielmehr muss bei der Umsetzung des DICOM-E-Mail-Standard auf die Einhaltung entsprechender Rahmenbedingungen geachtet werden. Wird Schlüsselerzeugung und Handhabung organisatorisch abgesichert, eine hinreichend starke Mindestschlüssellänge und sichere Algorithmen zur Umsetzung der Verschlüsselung und elektronischen Signatur zwingend vorgeschrieben, so werden Gesundheitsdaten mittels des Transportweges E-Mail sicherübertragen.

Kapitel 8 Conclusion

The DICOM E-Mail Standard uses e-mail as a medium for standard-compliant transmission of patient data. For health data protection, the data is encrypted according to the OpenPGP Standard.

According to standard specifications, the e-mail header data is transferred unencrypted. In particular, this includes the e-mail address of sender and receiver and the data specified in the subject line of an e-mail. The e-mail address of sender and receiver are mandatory for e-mail transmission, meaning they can hardly be protected via encryption.

Regarding the information given in the subject line of an e-mail, the DICOM E-Mail Standard does not cover the handling of this field. In particular no reference is available to the risks which are accepted when using the input field for personal health data. In the sense of a data protection friendly way, an extension of the standard is desirable so that

a) the risks of an unencrypted data transfer are referred to within the subject field;

b) DICOM E-Mail specifications regarding personal data exist for the use of the subject field.

The DICOM E-Mail Standard does not provide any specifications for using the encryption algorithm and key length. The OpenPGP Standard contains algorithms for encryption and an electronic signature that is considered save. However, from the present perspective this standard also contains algorithms that are considered unsafe and that do not ensure privacy.

For algorithms that are currently still considered save, it must be mentioned that their security also depends on the key length. As neither the DICOM E-Mail Standard nor the OpenPGP Standard define specifications relating to the key length or the algorithms to be used, a secure and insecure data transmission is, depending on use, possible via DICOM E-Mail Standard.

Neither the DICOM E-Mail Standard nor the OpenPGP Standard provides specifications for

- the generation of the key pair, necessary for the OpenPGP-compliant encryption (private and secret key),
- the storage and use of the key pair as well as
- the potential recall of the key pair.

Even with secure algorithms and a key length sufficiently strong, the security of encryption is critically dependant on how secure the key is that is used for encryption. Especially for health data considered among data with the highest level of data protection, the following is essential:

- The key pair is to be generated in such a way that only the authorized person receives the secret key, i.e. at no time a copy could be made for third parties.
- Storage and use of the private key take place in a way that only the authorized person has access to the private key.
- If the secret key is compromised, a recall is possible which prevents the unauthorized use of the access by third parties.

The sole conformant use of the DICOM E-Mail Standard does not guarantee secure data transmission. When implementing the DICOM E-Mail Standard, corresponding general conditions must be met.

In a scenario in which the key creation and use is founded from an organizational perspective, and a sufficiently strong minimum key length and secure algorithms are mandatory for the implementation of the encryption and the electronic signature, then health data is transmitted securely via E-Mail transmission.

Kapitel 9 Glossar

Authentifizierung	Die Authentifizierung bezeichnet den Vorgang, die Identität einer Person oder eines Rechnersystems anhand eines bestimmten Merkmals zu überprüfen. Beispiel: Benutzername/Passwort, Personalausweis
Authentizität	Unter dem Nachweis der Authentizität von elektronischen Daten versteht man den Nachweis über die Echtheit der Daten. Damit verbunden ist die eindeutige Zuordnung zum Verfasser, Ersteller und/oder Absender der Daten.
Elektronische Signatur	Entsprechend §2 Ziff. 1 Signaturgesetz (SigG) sind elektronische Signaturen „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Grundlage einer elektronischen Signatur ist ein Hashwert.
Hashfunktion	Eine Hashfunktion ist ein kryptographischer Algorithmus, bei dem Nachrichten beliebiger Länge auf einen Hashwert fester Länge abgebildet wird. Kryptographisch geeigneten Hashfunktionen weisen dabei zwei Eigenschaften auf: 1) Es ist praktisch unmöglich, zwei Nachrichten mit dem gleichen Hashwert zu finden (Kollisionsresistenz). 2) Bei einem gegebenen Hashwert ist keine Nachricht zu finden, die durch die Hashfunktion auf den Hashwert abgebildet wird (Einwegeigenschaft), d.h. ein Hashwert bildet genau eine Nachricht ab.
Integrität	Unter dem Nachweis der Integrität elektronischer Daten versteht man den Beweis, dass die Daten vollständig und unverändert sind.
OpenPGP	Pretty Good Privacy (PGP) ist ein von Phil Zimmermann entwickeltes Programm zur Verschlüsselung und zur Erzeugung digitaler Signaturen von Daten. OpenPGP basiert auf dem Format, welches mit PGP Version 5 eingeführt wurde, und ist im RFC 4880 standardisiert.
Public-Key-Infrastruktur (PKI)	Eine Public-Key-Infrastruktur (PKI) ist eine technische und organisatorische Infrastruktur, die es ermöglicht, kryptographische Schlüsselpaare (privater/öffentlicher Schlüssel) auszugeben und zu verwalten. Eine PKI besteht i.d.R. aus drei Instanzen: – Registrierungsinstanz – Zertifizierungsinstanz – Verzeichnisdienst
Secure Sockets Layer (SSL)	Secure Socket Layer (SSL) ist ein ursprünglich von der Firma Netscape entwickeltes Protokoll zur sicheren Übertragung von Daten in öffentlichen Netzen.
Transport Layer Security (TLS)	Transport Layer Security (TLS) ist ein Protokoll, welches die Kommunikation über ein öffentliches Netzwerk durch Datenverschlüsselung sichern und authentifizieren soll. TLS ist die Weiterentwicklung von SSL und bietet einige Verbesserungen hinsichtlich Sicherheit, Zuverlässigkeit und Interoperabilität.

Übersicht Begutachtung

Gegenstand	DICOM-E-Mail-Standardempfehlung der AG Informationstechnologie der Deutschen Röntgengesellschaft e.V.
Prüfungsart	Gutachten
Grundlage	Spezifikation der DICOM-E-Mail-Standardempfehlung in der Version 1.7
Zeitraum der Gutachten-Erstellung	01. Juni 2015 bis 07. August 2015
Berichtsdatum	07. August 2015
Auftraggeber	AG Informationstechnologie der Deutschen Röntgengesellschaft e.V.
Anschrift Auftraggeber	Ernst-Reuter-Platz 10 10587 Berlin
Ansprechpartner Auftraggeber	Prof. Dr. Thomas Hackländer Vorsitzender der AGIT
Gutachter	Dr. Bernd Schütze Leiter der Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V.
Ergebnis	Die vorgelegte Spezifikation ist geeignet, Gesundheitsdaten bei der Übertragung unter Nutzung des Mediums Internet hinreichend zu schützen. Allerdings nur, wenn durch organisatorische Vorgaben hinsichtlich Erzeugung und Handhabung der Schlüssel sowie bzgl. der zu nutzenden Algorithmen und Schlüssellängen gewährleistet ist, dass keine als unsicher anzusehende Handhabung des OpenPGP Standards erfolgen kann.