Düsseldorf, den 25. Juni 2014

Protokoll

der vierundzwanzigsten Sitzung des Ärztlichen Beirates

am Mittwoch, den 25. Juni 2014

in der Ärztekammer Nordrhein

in Düsseldorf

Vorsitz:	Dr. Christiane Groß, M.A., Dr. Dr. Hans-Jürgen Bickmann
Gast:	Matthias Redders (Ministerium für Gesundheit, Emanzipation, Pflege und Alter)
Anwesend:	s. Teilnehmerliste
Beginn:	15.00 Uhr
Ende:	17.00 Uhr

Hinweis: Aus Gründen der besseren Lesbarkeit wird in diesem Protokoll auf eine geschlechterdifferenzierte Formulierung verzichtet. Es wird ausdrücklich darauf hingewiesen, dass Begriffe wie Arzt, Patient, Mitglied usw. immer auch für die weibliche Form stehen, es sei denn, es wird ausdrücklich auf die männliche oder weibliche Form hingewiesen.

TOP 1 Begrüßung

Frau Dr. Groß begrüßt im Namen der beiden Vorsitzenden die Anwesenden (s. Teilnehmerliste).

Dr. Groß begrüßt den Referenten der heutigen Sitzung Herrn Frank Herrmann , Mitglied des Innenausschuss und Ausschuss für Kommunalpolitik des Landtag NRW. Die unter dem TOP 3.1 angekündigte Live Demonstration eines Hackerangriffs auf eine App in einem Mobil Devices muss leider auf Grund einer kurzfristigen Absage ausfallen.

Stattdessen werden Herr Matthias Redders vom Gesundheitsministerium, Herr Benno Herrmann von der gematik und Herr Hermann Abels-Bruns vom Projektbüro der ARGE eGK/HBA-NRW über den Stand des Erprobungsverfahrens ORS1 berichten.

TOP 2 Genehmigung des Protokolls der Sitzung vom 18. Dezember 2013

Dr. Groß ruft als nächsten Tagesordnungspunkt die Genehmigung des Protokolls der letzten Sitzung auf. Da keine schriftlichen Einsprüche vorliegen und auch in der Sitzung keine Beanstandungen angemeldet werden, wird das Protokoll in einer Abstimmung ohne Gegenstimmen und Enthaltungen angenommen.

TOP 3 Mobile Devices

Dr. Groß eröffnet den zentralen Tagesordnungspunkt der heutigen Sitzung, in dem es um die Nutzung von mobilen Geräten im Gesundheitswesen (Mobile-Health-Dienste) und den Gefahren bei ihrem Einsatz geht. Dazu begrüßt sie noch einmal Herrn Frank Herrmann, Sprecher für Privatsphäre und Datenschutz der Piratenfraktion im Landtag Nordrhein-Westfalen. Sie führt in das Thema ein, dass in der medizinischen Versorgung in Arztpraxen und Krankenhäusern mehr und mehr Mobilgeräte wie moderne Mobiltelefone mit leistungsfähigen Betriebssystemen und attraktiven Bandbreiten (z. B. iPhone), mobile Überwachungsgeräte oder sogenannte „persönliche digitale Assistenten“ (PDA, kompakt tragbare Computer wie z. B. das iPad) eingesetzt werden. Mobile-Health-Dienste können dazu beitragen, dass Gesundheitsleistungen effizienter und qualitativ besser erbracht werden und Informationen auch an entlegenen Arbeits- und Einsatzplätzen verfügbar gemacht werden. Dabei ist den Benutzern weitestgehend unklar, welchen Datenschutz- und IT-Sicherheitsrisiken sie sich dabei aussetzen. Hierüber soll der Vortrag von Herrn Herrmann aufklären. Die Folien des Vortrags werden dem Protokoll beigefügt.

Herrmann erläutert einige Anwendungsbeispiele von mobilem Computing wie z. B. Siri, einer Software von Apple, die der Erkennung und Verarbeitung von natürlich gesprochener Sprache dient und so Funktionen eines persönlichen Assistenten erfüllen soll. Die Sprachdaten werden bei bestehender Internetverbindung an einen Apple-Server übertragen, dort z. B. zu einem geschriebenen Diktat verarbeitet und das Ergebnis an das Endgerät zurückgemeldet. Siri soll, so Herrmann, die Daten für 2 Jahre speichern. Bei einem Einsatz im Gesundheitswesen können so sensible Daten in fremde Hände geraten. Aber auch auf anderen Wegen sind die vertraulichen Daten der Patienten auf mobilen Devices, aber auch auf stationären Geräten, die unzureichend geschützt und mit dem Internet verbunden sind, gefährdet. Dafür sind Spionage Apps und Trojaner verantwortlich, über die Geräte und ihre Funktionen manipuliert werden. Aber nicht nur Hacker, sondern auch staatlich organisierte Spionageorganisationen wie die NSA überwachen die weltweite Telefon- und Datenkommunikation. Obendrein können mobile Geräte leicht verloren gehen oder gestohlen werden, weshalb gespeicherte Daten auf diesen Geräten besonders geschützt sein müssen.

Nach jüngsten Schätzungen sind gegenwärtig 97.000 Mobile-Health- Apps (mHealth-Apps) über die verschiedenen Plattformen auf dem weltweiten Markt für die mobilen Geräte erhältlich. Da ist es für die Angehörigen der Gesundheitsberufe und Patienten schwierig, Apps nach fachlichen und gesetzlichen (Medizinproduktegesetz) Kriterien auszuwählen und Informationen über die Einhaltung von Datenschutzvorschriften und IT-Sicherheit zu erhalten. Das Auditorium möchte wissen, ob es eine Blacklist für Apps gibt, die Auskunft über die Vertrauenswürdigkeit gibt. Herrmann kennt keine solche Liste und verweist darauf, dass das bei insgesamt ca. 10 Mio. Apps weltweit auch kaum möglich ist. Ebenso ist nach seiner Meinung auch keine inhaltliche Eingrenzung dabei möglich. Es gibt zwar schon erste App-

Zertifizierungssysteme, aber niemand wird für diese Einordnung oder für Schäden beim Einsatz die Haftung übernehmen wollen.

Aus dem Auditorium wird darauf hingewiesen, dass die amerikanische Zulassungsbehörde FDA (Food and Drug Administration) Richtlinien festgelegt hat, wonach eine mHealth-App als Medizinprodukt einzustufen ist oder nicht.

Vorgaben und Überwachung zur Risikominimierung bei dem Einsatz von IT- und Kommunikationstechnologie im Gesundheitswesen werden u.a. durch den „Düsseldorfer Kreis“ erbracht. Dieser war bis 2013 eine informelle Vereinigung der obersten Aufsichtsbehörden, die in Deutschland die Einhaltung des Datenschutzes im nicht-öffentlichen Bereich überwachte. Er hatte sich nach dem Ort des ersten Treffens „Düsseldorfer Kreis“ genannt. Seit 2013 dient er als Gremium in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Kommunikation, Kooperation und Koordinierung der Aufsichtsbehörden im nicht-öffentlichen Bereich. In seinem Vortrag berichtet Herrmann von den hohen Datenschutz- und Sicherheitsanforderungen des „Düsseldorfer Kreises“ an im medizinischen Umfeld genutzten Netzwerken. Darin wird u. a. darauf verwiesen, dass der BÄK/KBV-Leitfaden zur Online-Anbindung von Praxis-EDV-Systemen eingehalten werden soll.

In diesem Zusammenhang verweist Herrmann auf die Ausführungen im „Grünbuch über Mobile-Health-Dienste (mHealth)“ der Europäischen Kommission, das dem Ärztlichen Beirat zugesandt wird. Außerdem wird der Link zum „Düsseldorfer Kreis“ den Mitgliedern des Ärztlichen Beirats übermittelt.

Die Vorsitzenden fokussieren das Gespräch noch einmal auf den zentralen Aspekt „Cloud Computing“ und möchten wissen, ob es Festlegungen zum Datenschutz und IT-Sicherheit bei Cloud Computing gibt. Hermann schränkt ein, dass die Sicherheit von „Cloud Computing“ nicht Sache eines Landesparlamentes ist, dessen Mitglied er ist, sondern in den Verantwortungsbereich des Bundes gehört. Sicherheit kann der Einzelne bei einer Kommunikation über das Internet nur erreichen, wenn er in seiner Kommunikation Verschlüsselungsverfahren einsetzt. Patientendaten dürfen deshalb immer nur verschlüsselt versendet werden und sein Netz muss man durch professionelle Schutzmaßnahmen vor Angriffen absichern. Andernfalls sind die Daten nicht zu schützen.

Viele Ärzte nutzen in ihren Praxen drahtlose Netzwerke, sogenannte W-LAN. Zunehmend muss der Arzt die Patientendaten aber auch vor Ort zur Verfügung haben. Dazu wird die Frage aus dem Auditorium nach vergleichbaren Sicherheitsstrukturen im W-LAN und bei der Nutzung von mobilen Devices gestellt. Welche Möglichkeiten gibt es, seine Daten in solchen Szenarien zu sichern?

Herrmann führt aus, dass für den Datenaustausch beschränkt auf Entfernungen innerhalb eines Gebäudekomplexes, wie zum Beispiel im Krankenhaus oder MVZ, WLAN-Funknetzwerke mit dem Funkstandard WiFi und der WPA2-Verschlüsselung zum Einsatz kommen. Dazu müssen die notwendigen Access Points eingerichtet und ausreichend gegen unautorisierte Benutzer abgesichert sein. Wegen der besonderen Gefährdung sollen solche Netzwerke nur von IT-Profis eingerichtet werden. Unterwegs, zum Beispiel beim Hausbesuch, nutzen Ärzte und Pflegekräfte zunehmend mobile Geräte, um Informationen abzurufen oder Daten elektronisch zu erfassen. Dazu dienen Smartphones und Tablet-PCs, wofür eine Mobilfunkverbindung benötigt wird. Zur Absicherung dieser Kommunikation empfiehlt er die Sicherheitsmaßnahmen, die BÄK und KBV in ihrem Leitfaden „Anforderungen an Hard- und

Software in der Praxis – Hinweise zum Datenschutz – Ein Leitfaden für Ärzte und Psychotherapeuten“ vorgegeben haben.

Seitens Mitglieder aus dem Krankenhausbereich wird auf das Gefährdungspotential hingewiesen, dass dadurch entstehen kann, dass Führungskräfte die Nutzung besonderer Anwendungen auf ihren mobilen Geräten durchsetzen, die sich außerhalb der Sicherheitspolicies ihrer IT-Abteilungen bewegen. Hier fehlen gesetzliche Vorgaben, um solche Gefährdungen zu verhindern.

Weiter wird seitens der Mitglieder darauf hingewiesen, dass es heute jedoch schon die Möglichkeit gibt, Smartphones und andere mobile Geräte durch Schutzsoftware sicher zu machen und dass das Angebot von sicherer Software und Apps zunehmen wird. Seitens der Anbieter Apple und Microsoft wird gefordert, sichere Betriebssysteme zur Verfügung zu stellen. Für die Sicherheit und den Schutz der Patientendaten in der Arztpraxis ist der Arzt verantwortlich. Es wird auf ein Urteil in Schleswig-Holstein verwiesen, wo es zu einer Verurteilung gekommen ist, weil die Internet-Anbindung unzureichend abgesichert war.

Zum Abschluss seines Vortrags fasste Herrmann seine Empfehlungen wie folgt zusammen:

- Es gibt eine überbordende Nutzung beim Internet und mobilen Anwendungen, jedoch hinkt die Sicherheit hinterher.
- Es gibt Anbieter von sicheren Mobiltelefonen, die teuer und nicht für den täglichen Einsatz zu gebrauchen sind.
- In Systemen und Software amerikanischer Hersteller gibt es absichtliche oder fehlerbedingte Lücken für unautorisierte Zugänge, die nicht nur von Geheimdiensten sondern auch von Marktteilnehmern wie Versicherungen genutzt werden.
- Wir benötigen offene Systeme (z. B. Open Source), die nicht von Gruppen kontrolliert werden und offen zugänglich für Testverfahren sind.
- Aufpassen! Aufpassen! Aufpassen!

TOP 3 Status des Erprobungsverfahren ORS1

Herr Hermann Abels-Bruns berichtet, dass der Aufbau des zentralen Netzwerkes der Telematikinfrastruktur planmäßig verläuft und bis zum Ende des Jahres 2014 abgeschlossen sein wird. Im Bereich der dezentralen Komponenten (Karten, Kartenterminals, Konnektor) wurden in Abstimmung mit den Gesellschaftern der gematik funktionale Erweiterungen und Verbesserungen in das laufende Verfahren eingebracht. Dieses führt zu einer Verzögerung des Beginns des Erprobungsverfahrens vom 4. Quartal 2014 voraussichtlich zum 2. Quartal 2015.

In dieser Verzögerung kann möglicherweise, so eine Einschätzung seitens der Mitglieder, eine Gefahr für die Akzeptanz des Projektes in der Ärzteschaft liegen. Nach den sehr kontroversen Debatten um die Einführung der eGK und der TI und der dünnen Mehrheit für eine weitere Beteiligung der Bundesärztekammer an der gematik und dem kommenden Erprobungsverfahren auf dem letzten 117. Deutschen Ärztetag in Düsseldorf muss man mit einer weiterhin kritischen Ärzteschaft auch auf dem kommenden 118. Deutsche Ärztetag in Frankfurt vom 12. – 15.05.2015 rechnen. Hätten nach altem Zeitplan positive Testergebnisse im

Vorfeld des Ärztetages den Befürwortern den Rücken stärken können, so ist durch die nun zu erwartende Verschiebung des Beginns des Erprobungsverfahrens ins 2. Quartal 2015 nicht mehr mit Testergebnissen zu rechnen, was eher den Gegnern zur Unterstützung ihrer Positionen nutzen kann.

Herr Mathias Redders berichtet über die Auseinandersetzung auf Bundesebene zur Einbindung des „Sicheren Netz der KVen“ (SNK) als Bestandsnetz an die Telematikinfrastruktur. Die KBV und KVen haben in den letzten Jahren mangels verfügbarer Alternativen, wie z. B. der Telematikinfrastruktur der gematik (TI), ein eigenes Netzwerk zum sicheren Austausch von Abrechnungs- und Gesundheitsdaten aufgebaut. Viele Pilotprojekte zu medizinischen Anwendungen in Nordrhein-Westfalen nutzen diese sichere Vernetzung, der auch vom Landesdatenschützer ein hinreichendes Sicherheitsniveau attestiert wird. Der Zugang in das SNK erfolgt über das Hardware basierte KV-SafeNet mittels eines VPN-Tunnelungsverfahrens. Dieses VPN erfüllt einen besonders hohen Sicherheitsstandard, da der Zugang nur mit festgelegten, speziell konfigurierten Zugangsgeräten (KV-SafeNet-Router) möglich ist. Deshalb ist es für Redders unverständlich, wie die gematik dieses Netz als unsicher bezeichnen kann und das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie die Bundesbeauftragte für den Datenschutz sodann fordern, dass dieses Netz vor seiner Anbindung als Bestandsnetz an die Telematikinfrastruktur von ihnen zugelassen und zertifiziert werden muss. Eine Forderung, die die KBV nach Meinung von Redders zu recht nicht akzeptieren kann. Alleine die in der Öffentlichkeit geführte Auseinandersetzung hierüber schadet der Reputation des Projektes.

Herr Benno Herrmann von der gematik (wird ab hier mit der Namensbezeichnung Herrmann in Abgrenzung zum Referenten zum TOP 2 Herrn Frank Herrmann dargestellt) führt aus, dass in den Arztpraxen, die am Erprobungsverfahren ORS1 teilnehmen und einen KV-SafeNet Router nutzen, dieser durch einen Konnektor der gematik ersetzt werde. Denn alle Ärzte wollen nur über einen Router arbeiten. Der Arzt erreicht über diesen Konnektor dann sowohl die TI als auch das SNK. Er hält diese augenblickliche Auseinandersetzung für positiv, da sie den Umfang der Optionen im Erprobungsverfahren deutlich mache und der Druck auf die Umsetzung des Projektes steige. Die Sicherheitsniveaus der TI und der SNK sind nicht gleich und deshalb muss das SNK auf das Sicherheitsniveau der TI angehoben werden. Der Arzt als Anwender soll keinerlei Einschränkungen bei der Auswahl seiner Anwendungen erfahren und die Anwendungen müssen entsprechend zertifiziert sein, unabhängig in welchem Netz sie sich befinden.

Abels-Bruns ist der Auffassung, dass die Attraktivität der TI in Zukunft dadurch steigt, dass auch Anwendungen angeboten werden können, die nicht in der TI angesiedelt sind. Die Einbindung einer Anwendung in die TI bedeutet, dass sie sich den umfangreichen Zulassungsbedingungen der gematik und des BSI unterwerfen muss. Befindet sie sich in einem externen Netz und wird über ein Gateway mit der TI verbunden, werden die Sicherheitsanforderungen in Richtung der TI in der Schnittstelle des Gateways zur TI spezifiziert. An das Sicherheitsniveau - und falls erforderlich - an die fachlichen und semantischen Schnittstellen der Anwendung im Netz des Betreibers wird die gematik ebenfalls Anforderungen definieren. Für den Nachweis der Umsetzung dieser Anforderungen sorgt aber der Betreiber eigenverantwortlich. Dadurch kann sich ein breites Angebot auch an konkurrierenden Anwendungen entwickeln und der Betreiber eines solchen Netzes behält die vollumfängliche Hoheit über sein Netz.

Aus dem Auditorium wurde in Richtung der gematik kritisiert, dass man mit derartig restriktiven Überlegungen den Ärzten das KV SafeNet zu nehmen versucht und man befürchtet, dass es dadurch in der Zukunft zu Einschränkungen hinsichtlich seiner Nutzung kommen kann. Der Arzt nutzt bisher KV SafeNet vor allem für seine Abrechnungen und das möchte er auch beibehalten. Mit Einführung der TI darf es für den Arzt aber nicht schwieriger werden, diese bestehende Anwendung neben Anwendungen der TI zu nutzen.

In einer weiteren Stellungnahme aus dem Kreise der Mitglieder wurde darauf hingewiesen, dass es bei der Kritik an der Einstellung der gematik zu KV SafeNet nicht darum geht, dass man unbedingt KV SafeNet erhalten möchte. Man braucht die darüber angebotenen Anwendungen nicht unbedingt; denn man kann auch immer noch offline arbeiten. Wichtigstes Kriterium für die Online Nutzung einer Anwendung ist der Nutzen, den sie dem Arzt bringen soll. Für den Arzt stellt die Entscheidung, seine Praxis online anzubinden, eine Schwellenüberschreitung dar, die nur durch den Zugewinn eines entsprechend hohen Nutzens für ihn in seiner Arbeitsqualität und Arbeitseffizienz zu rechtfertigen ist.

Die Ersetzung des KV SafeNet-Routers durch den Konnektor der TI steht, so eine weitere Stellungnahme aus dem Auditorium, nicht zur Disposition. Denn das Sicherheitsniveau des Konnektors und seine Sicherheitsfeatures seien erheblich höher und umfangreicher als z. B. die Verschlüsselungsverfahren und die „SignaturAnwendungsKomponente“ (SAK).

Herr Dr. Dr. Bickmann beendet diesen TOP, dankt den Referenten für Ihre Beiträge und äußert die Hoffnung, dass die Auseinandersetzung hoffentlich im Sinne einer zukunftsweisenden Nutzung der TI und des Bestandsnetzes der Ärzteschaft geregelt wird.

TOP 5 Verschiedenes

- Unter diesem Tagesordnungspunkt gibt es einige Vorschläge zu Themen für die nächsten Sitzungen des Ärztlichen Beirats:
    - Dr. Groß regt an, in der nächsten Sitzung das Thema „Identitätserfordernis von Patienten bei der Generierung von medizinischen Dokumenten“ zu erörtern. Hierzu hatte sie mit Herrn Dr. Holzborn und Herrn Zimmer einen Entschließungsantrag auf dem letzten Deutschen Ärztetag eingebracht, der vom Plenum beschlossen worden ist.
    - Redders schlägt vor, zur nächsten Sitzung einen Vortrag von Herrn Prof. Haas zum Thema „eHealth Standards, Interoperabilität und Nutzung eines Terminologieservers“ einzuplanen.
    - Frau Dr. Haferkamp empfiehlt für eine der nächsten Sitzungen, Herrn Neuhaus von der DKG zu einem Vortrag zu seinem Positionspapier zur eFA einzuladen.
    - Herr Düchting bietet zur Vertiefung des heutigen Vortrags zu „Mobile Devices“ an, noch eingehender über Risiken beim Einsatz solcher mobilen Komponenten zu referieren. Er ist wegen seines Urlaubs erst jedoch zur übernächsten Sitzung verfügbar.

- Die nächsten Termine:
    - Die Vorbesprechung zum nächsten Ärztlichen Beirat ist am Mittwoch den **30. Juli 2014** um 20:00 Uhr in der Ärztekammer Nordrhein in Düsseldorf.
    - Die nächste Sitzung des Ärztlichen Beirats ist nicht wie ursprünglich geplant am 20. August 2014 bei der KV WL in Dortmund, sondern sie wird auf besonderem Wunsch von Herrn Redders am Mittwoch den **17. September 2014 um 15:00 Uhr innerhalb der Veranstaltung IT-Trends auf dem Messegelände der Messe Essen abgehalten.**