24. März 2021

Protokoll
der 63. Sitzung des Ärztlichen Beirates Digitalisierung in Nordrhein-Westfalen am Mittwoch, den 24. März 2021 per Videokonferenz

Vorsitz:	Dr. Christiane Groß, M.A., Dr. Dr. Hans-Jürgen Bickmann
Protokoll:	Lisa Schockenhoff, ZTG GmbH
Gäste:	Herr Holm Diening (Leiter Informationssicherheit und Datenschutz, gematik) Herr Lars Gottwald (Leiter Business Teams, gematik) Herr Martin Tschirsich (Information Security Consultant, CCC) Herr Dirk Schladweiler (Dezernat 5 Digitalisierung im Gesundheitswesen, Bundesärztekammer) Herr Peter Vahrenhorst (Stv. Sachgebietsleiter, Cybercrime Kompetenzzentrum, Landeskriminalamt NRW)
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

Die Vorsitzende Frau Dr. Groß begrüßt die Referenten der heutigen Sitzung, sowie die anwesenden Mitglieder und Gäste.

TOP 2 Genehmigung des Protokolls der Sitzung vom 20. Januar 2021

Am Protokoll wurden nachträglich zwei kleinere redaktionelle Änderungen vorgenommen. Es wird daher im Nachgang der Sitzung erneut zur Abstimmung versandt.

TOP 3 Aktueller Sachstand zur Einführung der Telematikinfrastruktur (Herr Lars Gottwald)

Herr Gottwald berichtet zum aktuellen Sachstand zur Einführung der Telematikinfrastruktur.

Im Januar wurde von der gematik ein Whitepaper mit dem Titel „TI 2.0 – Arena für digitale Medizin“ veröffentlicht (s. https://www.gematik.de/fileadmin/user_upload/gematik/files/Presseinformationen/gematik_Whitepaper_Arena_digitale_Medizin_TI_2.0_Web.pdf). Hierin wird ein Ausblick auf die Planungen zur zukünftigen

Ausrichtung und Weiterentwicklung der Telematikinfrastruktur gegeben. Ein öffentlicher Diskurs des Papiers und der hierin dargelegten Themen ist ausdrücklich erwünscht. Der Auftakt hierzu wurde am 10. März mit dem „TI-Future Summit“ gemacht. Bis zum Sommer sollen weitere Veranstaltungen folgen und der Dialog zur Gestaltung des Whitepapers fortgeführt werden. Ziel ist es bis September 2021 mit einer abgestimmten gemeinsamen Zielvorstellung zur Weiterentwicklung der Telematikinfrastruktur aus dem Diskurs hervorzugehen. Ganz grundsätzlich soll mit der TI 2.0 unter Beibehaltung eines angemessen hohen Sicherheitsniveaus die Komplexität in den Leistungserbringerumgebungen verringert werden.

KIM

Bisher haben acht KIM-Dienste eine Zulassung der gematik erhalten.

Die Zahl der angeschlossenen KIM-Nutzer bewegt sich aktuell im niedrigen vierstelligen Bereich.

eRezept

Die Einführung des eRezepts ist zum 30.06.2021 geplant. Bis zu diesem Zeitpunkt soll auch die Komfortsignatur verfügbar sein. In der Testregion Berlin ist eine begleitende Einführung des eRezepts vorgesehen. Verpflichtend wird die Nutzung ab dem 01.01.2022.

eAU

In der Gesellschafterversammlung am 23.03.2021 wurde beschlossen vor der offiziellen Einführung der eAU am 01.10.2021, vom 01.06.2021 bis zum 31.08.2021 mit den Gesellschaftern einen Feldtest zur Einführung der eAU durchzuführen.

eHBA

Schlüssel für den Zugang zu den digitalen Anwendungen der Telematikinfrastruktur ist der Heilberaufsausweis. Stand 24.03.2021 wurden ca. 77.000 Ausweise an niedergelassene Ärzte, Krankenhäuser und Apotheken ausgegeben.

ePA

Nach erfolgreich beendeter Testphase der ePA soll der Rollout im 2. Quartal 2021 beginnen und wird eng von der gematik begleitet werden. Die flächendeckende Vernetzung von Arztpraxen, Krankenhäusern und Apotheken wird dann für die Quartale Q3 und Q4 2021 erwartet.

DEMIS

Im Rahmen der Pandemie-Bekämpfung unterstützt die gematik das RKI im Kontext DEMIS. Alle Gesundheitsämter wurden zum 01.01.2021 angebunden und 375 Labore melden zurzeit bereits aktiv an DEMIS. Seit Ende 2020 besteht zudem eine Schnittstelle zu SORMAS. In diesem Jahr ist außerdem noch die Einrichtung eines Meldeportals für Leistungserbringer geplant.

offene, standardisierte Schnittstellen für informationstechnische Systeme

Die gematik wurde vom Gesetzgeber beauftragt verbindliche Standards für den Austausch von Gesundheitsdaten mit Informationssystemen im Krankenhaus zu erarbeiten. Um den intersektoralen Datenaustausch zu standardisieren wurden Datenobjekte nach dem FHIR-Standard festgelegt. Die definierten Datenobjekte befinden sich

gerade im Kommentierungsverfahren. Die KBV legt MIOs und die standardisierten Schnittstellen für den Datenaustausch mit PVS-Systemen fest. Zwischen der KBV und der gematik findet eine enge Abstimmung statt, um auch hier Interoperabilität durch abgestimmte Festlegungen sicherzustellen.

In der anschließenden Diskussion wird die Einbindung des ÖGD in die Telematikinfrastruktur thematisiert. Zu diesem Thema finden derzeit Gespräche mit den Vertragsparteien zur Finanzierung des Anschlusses statt. Informationsveranstaltungen für die Gesundheitsämter sollen durchgeführt werden. Frau Dr. Martina Franzkowiak empfiehlt zur Abstimmung eine Kontaktaufnahme mit der Akademie des ÖGD.

Zur Unterstützung der Leistungserbringer beim Anschluss an die Telematikinfrastruktur stehen im gematik Fachportal Leitfäden zur Verfügung. Auch für die Anbindung der Krankenhäuser wurde ein Leitfaden erstellt. Herr Gottwald sagt zu, diesen im Nachgang der Sitzung zur Verfügung zu stellen. Er wird dem Protokoll als Anlage beigefügt (s. Anlage 1). In der nächsten vorbereitenden Sitzung des Ärztlichen Beirats soll das Thema „Softwarekonnektor“ thematisiert werden.

Zum Thema HBA erfolgt der Hinweis, dass die Nutzung der elektronischen Signatur bisher nicht überall problemlos möglich ist und auch regelmäßig durchgeführte Updates bisher keine Abhilfe des Problems schaffen konnten.

TOP 4 Datensicherheit in der Telematikinfrastruktur

Die Datensicherheit in der TI wird aus drei verschiedenen Perspektiven beleuchtet.

4.1 aus Sicht der gematik (Herr Holm Diening)

Herr Diening ist seit 2012 bei der gematik angestellt und beschäftigt sich seit 1999 mit dem Thema Datensicherheit.

Er berichtet anhand einer Präsentation (s. Anlage 2) zum Thema Datensicherheit aus Sicht der gematik.

Es gab in der Vergangenheit Beispiele für erfolgreich ausgeführte Hackerangriffe auf Systeme in denen Patientendaten hinterlegt waren. Alle Fälle haben gemeinsam, dass die Speicherung der Daten in diesen Systemen zentral erfolgte und ein zentraler Administrator vorhanden war.

Innerhalb der TI bzw. innerhalb der ePA gibt es keine Akteure mit Vollzugriff und ausgetauschte Daten werden Ende-zu-Ende verschlüsselt. Der größte Unterschied zu anderen Systemen besteht demnach darin, dass es keine „Super-User-Rolle“ gibt. Zugriffsprotokolle erlauben außerdem eine Nachvollziehbarkeit der Zugriffe auf die ePA. Dies erleichtert auch die Einhaltung des Prinzips der Datensparsamkeit und trägt zur DSGVO-konformen Gestaltung der Akte bei.

In der TI-2.0 sollen einige Sicherheitsmechanismen anders gelöst werden als bisher. Die TI wird dadurch so umstrukturiert, dass die Funktionen des Konnektors entweder nicht mehr benötigt werden oder an andere Stellen verlagert werden können. Die Umstellung wird schrittweise erfolgen. Die Sicherheitsarchitektur wird maßgeblich auf dem Prinzip des Zero-Trust-Networkings basieren. Ein Zugriff auf das Netzwerk wird für jede einzelne Zugriffsanfrage erst nach Authentifizierung des Nutzers erlaubt. Das implizite Vertrauen das dem geschlossenen Netz (VPN) entgegenbracht wurde, wird ersetzt und dadurch auch kein geschlossenes Netz mehr benötigt. Dies erlaubt auch die Nutzung von marktgängigen IT-Sicherheitskomponenten. Auf der Leistungserbringerseite ergibt sich durch den Wegfall der Notwendigkeit zur Integration der Technik in

der eigenen Praxis eine deutliche Reduzierung des Aufwands und der Komplexität der Implementierung.

Für Ende des Jahres 2021 ist ein Hacker-Contest auf einer Kopie des eRezeptes geplant.

Fragen an Herrn Dienig können im Nachgang der Sitzung gerne schriftlich per Mail an Herrn Christopoulos eingereicht werden.

4.2 aus Sicht des Chaos Computer Clubs (CCC) (Herr Martin Tschirsich)

Herr Tschirsich ist unabhängiger und freiberuflicher IT-Sicherheitsberater und spezialisiert sich durch seine Arbeit beim CCC u.a. auf das Thema Digitalisierung im Gesundheitswesen.

Der CCC konnte insbesondere zwei Schwachstellen für Angriffe auf die Telematikinfrastruktur ermitteln:

- Angriff auf den Vertrauensraum: Im Dezember 2019 gelang Hackern des CCC die Beschaffung von Ausweisen und Konnektoren über die Identitäten Dritter und erhielten so Zugriff auf Patientendaten der Telematikinfrastruktur. Es hat sich gezeigt, dass ein Vertrauensraum unentbehrlich ist. Benötigt werden sichere digitale Identitäten und eine sichere Authentisierung.
- Angriff auf die dezentrale Umgebung: Ende des Jahres 2020 konnten Mitglieder des CCC eine weitere Schwachstelle, diesmal in der Praxisumgebung in den LE-Institutionen selbst entdecken. Stellenweise war der VPN-Zugangsdienst unzureichend konfiguriert worden, sodass ein Zugriff von außen über den Konnektor auf Patientendaten möglich war.

Herr Tschirsich weist darauf hin, dass die in der IT-Sicherheitsrichtlinie beschriebenen Anforderungen aus seiner Sicht nicht ausreichend sind, um die Sicherheit in der dezentralen Leistungserbringerumgebung ausreichend zu gewährleisten. Auch eine vollständige Umsetzung der Richtlinie ist demnach nicht ausreichend, um den Schutz von Patientendaten umfänglich zu gewährleisten und Ärzte aus der Haftung zu nehmen. Benötigt werden insbesondere Finanzierungsregelungen, die die Kosten für die notwendigen Maßnahmen zur Einrichtung eines angemessenen IT-Sicherheitsniveaus abdecken können.

Weiterhin betont wird die hohe Relevanz des Einsatzes einer Ende-zu-Ende-Verschlüsselung bei der Datenübertragung insbesondere auch für die TI 2.0. Bei echter Ende-zu-Ende-Verschlüsselung müssen die Endgeräte selbst angegriffen werden, da innerhalb der übertragenden Struktur keine Zugriffsmöglichkeiten von außen bestehen. Der ePA fehlt diese echte Ende-zu-Ende-Verschlüsselung bisher.

Zusammenfassend kann gesagt werden, dass insbesondere im Vertrauensraum der TI ein Kernstück sicherer Digitalisierung im Gesundheitswesen gesehen werden kann. Schlüsselkomponenten dieses Vertrauensraumes sind Digitale Identitäten wie sie das DVPMG vorsieht. Auch wenn sich die Authentifizierung mittels Video-Ident momentan als Standard im Gesundheitswesen etabliert, sollte mit der Nutzung nicht leichtfertig umgegangen werden. Der BfDI und das BSI warnen vor den Gefahren der Nutzung und der BfDI empfiehlt ausdrücklich darauf zu verzichten bzw. bezeichnet das Video-Ident-Verfahren als nicht zulässig. Das liegt insbesondere an den leicht umzusetzenden Manipulationsmöglichkeiten eines Ausweises.

Relevante Bedrohungen gehen insbesondere von der Leistungserbringerumgebung aus. Insbesondere eine sinnvolle Weiterentwicklung der IT-Sicherheitsrichtlinie sollte daher erwogen werden.

Fragen an Herrn Tschirsich können im Nachgang der Sitzung schriftlich per Mail an Herrn Christopoulos eingereicht werden.

4.3 im Kontext der Cyberkriminalität (Herr Peter Vahrenhorst)

Herr Vahrenhorst ist Kriminalhauptkommissar beim LKA NRW und am Cybercrime-Kompetenzzentrum für das Thema Prävention von Cyberkriminalität zuständig.

Er beleuchtet über das Thema Datensicherheit in der Telematikinfrastruktur im Kontext der Cyberkriminalität anhand einer Präsentation. (s. Anlage 3).

Über das Internet wird in den unterschiedlichsten Bereichen kommuniziert. 2020 gab es weltweit 30 Milliarden vernetzte digitale Endgeräte – für 2024 wird eine Verdopplung auf 62 Milliarden digitalen Endgeräten erwartet. Hierunter sind nicht nur Smartphones zu verstehen, sondern alle Geräte die in irgendeiner Art und Weise mit dem Internet verbunden und Daten austauschen können (Saugroboter, Blutdruckmessgeräte, …). Auch das Risiko für Angriffe auf diese Infrastrukturen wird dadurch immer größer.

Erst kürzlich hat ein Hackerangriff auf das Uniklinikum Düsseldorf zu einem mehrwöchigen Ausfall der IT-Systeme und damit zu weitreichenden Einschränkungen der Patientenversorgung geführt.

Das Verständnis für die technische Zusammenhänge die Hackerangriffe erst ermöglichen ist wichtig – trotzdem sollte bei der Umsetzung von Maßnahmen zur IT-Sicherheit auf Spezialisten vertraut werden. Kooperationen der zuständigen Einrichtungen und Verbänden aus Forschung, Lehre und Industrie mit den Strafverfolgungsbehörden wird als sinnvoll erachtet, um aus den Fehlern anderer zu lernen und diese bei den Planungen von IT-Sicherheitsmechanismen zu berücksichtigen.

Fragen an Herrn Vahrenhorst können im Nachgang der Sitzung schriftlich per Mail an Herrn Christopoulos eingereicht werden.

TOP 5 Verschiedenes

Es besteht kein weiterer Diskussionsbedarf.

Die nächsten Termine:

- Die Vorbesprechung zum übernächsten Ärztlichen Beirat findet am Mittwoch den 28. April 2021 um 20:00 Uhr per Videokonferenz statt.
- Die nächste Sitzung des Ärztlichen Beirats findet am Mittwoch den 26. Mai 2021, um 15:00 Uhr per Videokonferenz statt.