



### **TOP 3 Zwischenbilanz und Ausblick der Arbeit des Ärztlichen Beirates**

Aufgrund der Überlegung im Vorfeld wurde eine Tischvorlage als Diskussionsgrundlage entwickelt, die jedoch aus organisatorischen Gründen leider zu kurzfristig fertiggestellt werden konnte. Daher konnten sich die Mitglieder des Beirats nicht ausreichend vor der Sitzung damit befassen. Der TOP wird zurückgestellt, um nach TOP 5 – falls ausreichend Zeit dazu ist – besprochen zu werden.

→ Aufgrund der vorangegangenen Diskussionen und der fortgeschrittenen Zeit wird der TOP auf die nächste Sitzung verschoben.

### **TOP 4 Lastenhefte (Gematik-Gesellschafterversammlung am 25. März 2011)**

Fr. Dr. Groß fasst den Schriftverkehr mit dem Schlichter zusammen (s. Tischvorlage).

Es besteht noch Unsicherheit bei der Interpretation des Briefes bezüglich folgender Formulierung: *„Gemäß dem beschlossenen Richterspruch zum Thema Selektivverträge wird es auch zukünftig möglich sein, dass der Arzt zur Behandlung von Versicherten mit Selektivverträgen nicht zwangsläufig aus seinem Praxisverwaltungssystem online auf Daten zugreifen muss, um vertragskonform handeln zu können. Dem Arzt wird der Zugang zu den notwendigen Informationen auch auf konventionellem Wege ermöglicht.“* Als konventioneller Weg könnte hier die Information über Brief, Fax oder Telefonat gemeint sein, was jedoch von Seiten der Ärzte als eingeschränkt praktikabel gesehen wird.

Die Themen zum Notfalldatenmanagement (z. B. Kosten der ausreichenden Schulung von Patienten und Ärzten, Finanzierung des Gutachtens über die Haftungsfragen) konnten noch nicht abschließend geschlichtet werden. Sobald ein Konsens gefunden ist, wird der Ärztliche Beirat darüber in Kenntnis gesetzt.

#### **TOP 4.1 Lastenheft Versichertenstammdatenmanagement**

Herr Dr. Christian Ummerle (s. Anlage)

Herr Dr. Ummerle berichtet über den aktuellen Entwicklungsstand des Versichertenstammdatenmanagements (VSDM) unter Federführung des GKV-Spitzenverbands. Das Lastenheft wurde in der Gesellschafterversammlung der gematik am 25. März 2011 verabschiedet. Aktuell finden die Arbeiten zur Lösungsanalyse und zum Konzept- sowie Spezifikationsdesign im Rahmen der Pflichtenhefterstellung statt.

Die obersten Ziele sind die Wirksamkeitsreife der Anwendung sowie die Nutzung bestehender und bereits getesteter Komponenten und Dienste. Mit der Neuausrichtung des Projektes und der damit einhergehenden Ende-zu-Ende-Verantwortung der federführenden Organisationen für die entsprechenden Anwendungsprozesse sollen nun auch der Datenschutz und sicherheitsrelevante Anforderungen an einem zielgerichteten Sicherheitsniveau für das VSDM ausgerichtet werden. Dies kommt der Umsetzung von Anforderungen zur Praxistauglichkeit entgegen. Zuvor orientierten sich die Sicherheitsanforderungen aller Anwendungen gleichermaßen an den Maximalforderungen. Weitere Kernthemen sind die Komplexitätsreduzierung, die Optimierung der Performance der Anwendung und die Berücksichtigung der neuen Anforderungen aus dem SGB V.

Die Onlineprüfung und -aktualisierung der eGK erfolgt mindestens mit jeder erstmaligen Inanspruchnahme von Leistungen im Quartal gemäß § 291 2b SGB V. Sie ist mit dem BSI abgestimmt und umfasst die Prüfung der Gültigkeit der eGK (offline oder online), der Aktualität der Daten auf der eGK sowie das Aktualisieren der Daten auf der eGK, sofern aktuelle Daten durch den Kostenträger bereit stehen. Der Prüfnachweis wird für Abrechnungszwecke gem. § 295 2b SGB V erzeugt und im Online-Szenario direkt an das PVS übergeben, im Stand-alone-Szenario zu späteren Übertragung an das PVS auf der eGK gespeichert. Er wird auch bei Nichtverfügbarkeit der Telematik-Infrastruktur erzeugt und bestätigt die Leistungspflicht. Ein Missbrauch durch eine ungültige eGK im Falle einer Überweisung ist auch bei einem derart generierten positiven Prüfnachweis ausgeschlossen, da die Karte bei Erstbesuch eines Arztes neu geprüft wird.

Für die Richtigkeit der Versichertenstammdaten sind die Kostenträger verantwortlich. So sollte beispielsweise eine Namenskorrektur idealerweise beim Kostenträger durchgeführt und dann nach dem Online-Abgleich der eGK in das PVS übernommen werden.

Zur Abbildung der Selektivverträge auf der eGK wurde in der letzten Gesellschafterversammlung am 26. Juni 2011 folgendes beschlossen:

- Auf der eGK wird jeweils eine Kennzeichnung für ärztliche und zahnärztliche Selektivverträge verbindlich eingeführt. Diese Kennzeichnung kann die Ausprägung „ja“, „nein“ oder „nicht genutzt“ erhalten.
- In der Testphase können die Krankenkassen im geschützten Bereich die Paragraphen des SGB V, in denen Selektivverträge beschrieben sind, abbilden, wenn der Versicherte ausreichend aufgeklärt wurde und dies schriftlich bestätigt.
- Die Kostenträger entwickeln einen Dienst, um für jeden befugten Arzt die notwendigen Informationen aktuell online oder auf konventionellem Weg ohne eine Profilbildung bereitzustellen.

Im Sinne der Verbesserung der Performance, der Reduktion der Komplexität und der Datensparsamkeit entfällt die Rollenprüfung bei der Online-Aktualisierung der VSD sowie die Signatur des Datenbearbeiters. Dadurch ist keine Anonymisierung des Datenbearbeiters beim Intermediär/Broker (vgl. Folie 10 der Anlage) mehr notwendig. Die Anonymisierung der IP-Adresse des Datenbearbeiters bleibt bestehen.

Auf der eGK werden die letzten 50 Arztbesuche zum Zweck der Datenschutzkontrolle protokolliert. Die Versicherten dürfen diese Daten einsehen; die Ärzte dürfen auf diese Protokoll-daten aus Datenschutzgründen nicht zugreifen. Es wird ausdrücklich darauf hingewiesen, dass die Kostenträger auch hieraus keine Profile erstellen können.

#### **TOP 4.2 Lastenheft Basis TI**

Herr Dirk Drees, Herr Wilhelm Haupt (s. Anlage)

Die Herren Drees und Haupt berichten über den aktuellen Entwicklungstand der Basis Telematik-Infrastruktur (Basis TI) unter der gemeinsamen Federführung des GKV-Spitzenverbands und der Kassenärztlichen Bundesvereinigung. Das Lastenheft wurde in der Gesellschafterversammlung der gematik am 25. März 2011 verabschiedet. Da es keine (klassische) Auftraggeber-Auftragnehmer-Beziehung gibt, findet auch keine personelle Tren-

nung zwischen Lasten- und Pflichtenheftphase statt. Ebenso wie beim VSDM teilt sich die Pflichtenhefterstellung für die Basis TI in die beiden Phasen Lösungsanalyse und Design. Die Spezifikationen des Pflichtenhefts reichen über die Testdurchführung hinaus bis in den Produktionsbetrieb. Die Basis TI (auch TI-Plattform) bezeichnet alle zentralen Dienste und dezentralen Komponenten (eGK, HBA, SMC) der TI. Die fachanwendungsspezifischen Dienste und Module gehören nicht in den Bereich der Basis TI.

Der Bestandsschutz betrifft in diesem Projekt zentrale Dienste, die von der gematik beauftragt wurden, sowie dezentrale Komponenten, für die bereits Zulassungsverfahren initiiert wurden (eGK, HBA, SMC, BCS-Kartenterminals, mobile Kartenterminals der Stufe 1). Änderungen an diesen Spezifikationen werden im weiteren Verlauf nach wirtschaftlichen Gesichtspunkten bewertet.

Trotz der jeweiligen Ende-zu-Ende-Verantwortung der federführenden Organisationen wird durch die Verwendung einheitlicher Methoden zum Datenschutz und zur Informationssicherheit sichergestellt, dass aus den Einzelementen der TI ein datenschutzkonformes und sicheres Gesamtsystem entstehen kann. Für die koordinierte Weiterentwicklung der TI sowie die Neueinführung von Anwendungen sorgt ein übergreifendes Releasemanagement gemeinsam mit einer Nutzungspolicy, mit einem nachgelagerten übergreifenden Test- und Migrationskonzept. Bis in die Erprobungsphase des Wirkbetriebs hinein können Fehler noch verhältnismäßig aufwandsarm behoben werden.

Es ist keine sektorale Trennung der Broker vorgesehen, wie sie in früheren Konzepten beschrieben wurde.

Die Anbieter von Komponenten und Dienste der TI nehmen die Betriebsverantwortung weitestgehend selbst wahr. Die Gesamtverantwortung für den Betrieb der TI liegt bei der gematik als Betreibergesellschaft, jedoch nicht im Sinne eines Echtzeitmonitorings. Über eine entsprechende Dokumentation und Protokollierung werden Prozesse, auch für Haftungsfragen, nachvollziehbar. Zielgrößen für die Umsetzung der Betriebsverantwortung sind die Aufrechterhaltung eines zuverlässigen Betriebes sowie die Wahrung der Marktoffenheit und der Diskriminierungsfreiheit.

Aktuell werden die Grobkonzepte für Architektur, Test und Betrieb erstellt und mit den Fachprojekten abgestimmt sowie Methoden zur Informationssicherheit und zum Datenschutz erarbeitet. Eine Fertigstellung und Abstimmung der Ergebnisdokumente der Lösungsanalyse ist für das 3. Quartal 2011 geplant.

Die operative Umsetzung des Testbetriebs ist in den Testregionen vorgesehen, allerdings in weitaus größerem Umfang als in den vergangenen Feldtests, um aussagefähige Ergebnisse zu bekommen. In einem gemeinsamen Gespräch mit den Testregionen werden die genauen Randbedingungen erst noch festgelegt.

Ob eine Praxis durch den Online-VSDD angreifbar wird, hängt in erheblichem Maße von der technischen Betreuung und damit der Sicherheit des Systems ab und liegt in der Verantwortung des Praxisinhabers. Ausgehende Nachrichten werden grundsätzlich anonymisiert (keine Profilbildung möglich). Die Kostenträger dürfen keine Arzt-Patienten-Profile erstellen. Zum Schreiben von Daten auf die eGK wird eine gesicherte Verbindung genutzt.

Eine Untersuchung der Performance des Online-VSDD ist vorgesehen. Nach aktuellen Informationen wird davon ausgegangen, dass die Lesezeiten der eGK in 98 % der Fälle unter 5 sek. liegen werden.

Die Referenten stellen sich den Fragen der Mitglieder des Beirates, noch offene Fragen zu den Projekten können per E-Mail an Fr. Dr. Groß gerichtet werden. Sie wird diese gesammelt an die Projektleiter weiterleiten mit der Bitte um Beantwortung.

Die Vorsitzenden des Ärztlichen Beirats mahnen an, zeitnah in die laufenden Prozesse eingebunden zu werden und rechtzeitig Einsicht in die relevanten Dokumente zu erhalten. Hierbei wäre eine verständliche Zusammenfassung und ggf. auch die Übersetzung der zugrundeliegenden Techniken für den technischen Laien Arzt wünschenswert.

Laut Auskunft der Herren Dr. Ummerle, Drees und Haupt findet im Juli ein Gespräch statt, in dem das weitere Vorgehen zu den Implementierungsleitfäden abgestimmt wird. Ärzte werden dort nach Aussage der Projektleiter einbezogen.

## **TOP 5 Nutzung von e-Health-BCS-Lesegeräten**

Herr Kowalski, BSI, erläutert den Sachstand zu den vermeintlichen Sicherheitsmängeln der eHealth-BCS-Lesegeräte bei der PIN-Eingabe, die in den Medienberichten Ende Mai beschrieben wurden, sowie die Anforderungen des BSI zur sicheren Einsatzumgebung.

Technisch ist die sogenannte Schwachstelle dadurch bedingt, dass die Kartenterminals über zwei Betriebsmodi verfügen: einen gesicherten Modus für die Eingabe der PIN sowie einen ungesicherten Modus, wie er u. a. für administrative Aufgaben genutzt wird. Im letztgenannten Modus könnte ein Angreifer missbräuchlich zur Eingabe der PIN auffordern.

Der derzeitige Einsatz der eHealth-BCS-Kartenterminals im Basis-Rollout verlangt weder die Eingabe einer PIN noch die Eingabe von sonstigen Daten zur Anwendungssteuerung. Zu einem späteren Zeitpunkt, zur Nutzung der Online-Anwendungen, muss das eHealth-BCS-Terminal durch ein Software-Update zu einem sogenannten eHealth-Terminal aktualisiert und an einen Konnektor angeschlossen werden, der dann einen Missbrauch ausschließt.

Manche eHealth-BCS-Terminals können bereits heute im Sinne des Signaturgesetzes als Signatur-Chipkartenlesegerät für die Verwendung qualifizierter elektronischer Signaturen (QES) eingesetzt werden, z. B. zur Abrechnung in Verbindung mit dem elektronischen Arzt ausweis. Diese Anwendung macht eine PIN-Eingabe erforderlich. Im sicheren Eingabemodus kann eine PIN gefahrlos eingegeben werden. Eine missbräuchliche Manipulation ist nicht möglich und die PIN verlässt das Kartenterminal nicht. Der sichere Eingabemodus wird durch eine LED-Anzeige oder ein Schlosssymbol im Display des Terminals angezeigt. Solange der sichere Eingabemodus nicht signalisiert wird, darf keine PIN eingegeben werden.

Wenn ein für den Basis-Rollout zugelassenes eHealth-BCS-Kartenterminal für qualifizierte elektronische Signaturen (QES) genutzt wird, gelten nach SiG/SigV zusätzlich besondere Anforderungen an die Einsatzumgebungen. Beispielsweise hat die Anwendung der QES in einem „geschützten Bereich“ zu erfolgen, in dem der Signaturkarteninhaber das Kartenterminal dauerhaft unter seiner alleinigen Kontrolle hat.

Auch der regelrechte Einsatz der eHealth-BCS-Kartenterminals im Basis-Rollout orientiert sich gemäß BSI an bestimmten Randbedingungen. U. a. ist das Terminal in angemessenen Intervallen auf Unversehrtheit zu prüfen (z. B. Sichtprüfung der Siegel). Diese Vorgabe basiert auf der Anforderung, dass die Terminals herstellerseitig durch Siegel, Öffnungs- und Durchbruchüberwachungen vor Manipulationen geschützt sind, so dass Manipulationen, für die maximal das o. g. Zeitfenster zur Verfügung steht, mit hoher Wahrscheinlichkeit erkannt werden.

Die von Seiten des BSI formulierten Einsatzbedingungen orientieren sich an den bisher zugrunde gelegten Betriebsrandbedingungen. Herr Kowalski betont an dieser Stelle die Notwendigkeit eines in der Ärzteschaft abgestimmten Betriebskonzepts unter Federführung der Bundesärztekammer, welches die realen Randbedingungen in der Einsatzumgebung der Kartenterminals beschreibt. Ein solches Betriebskonzept soll durch den Ärztlichen Beirat eingefordert werden. Dazu wird in einer der nächsten Sitzungen ein entsprechender Entwurf erarbeitet.

## **TOP 6    Verschiedenes**

### **Top 6.1    Aktueller Stand des eGK-Rollout**

Laut Auskunft der Kostenträger kann in Nordrhein-Westfalen mit der Ausgabe von ca. 3 Mio. eGKs – d. h. mit dem überwiegenden Anteil – bis zum Jahresende gerechnet werden. Die Ausgabestrategien der verschiedenen regionalen und überregionalen Kassen sind hierbei unterschiedlich. Nach Aussage der Kassenvertreter sind bereits Informationen über die kas-seneigenen Kundenmagazine und Internetseiten an die Versicherten ergangen. Auch eine individuelle Information der Versicherten soll noch folgen. Die Bildbeschaffung läuft z. T. schon über die Möglichkeit des Online-Uploads von Fotos.

Der ärztliche Beirat mahnt hier eine ausreichende Information der Patienten schon bei der Ausgabe der eGK an, damit nicht der Beratungsaufwand letztendlich in der Arztpraxis aufgefangen werden muss. Auch muss nach Meinung der Ärzteschaft die Übereinstimmung der angegebenen Daten mit den Daten des Versicherten durch die Kostenträger vor Ausgabe der eGK überprüft werden.

### **Top 6.2    Lichtbildbeschaffungsprozess**

Die Herren Dietrich, Stagge und Dr. Wollring beantragen einen Beschluss zur Authentifizierung der Lichtbilder der Versicherten durch die Kassen. Sie kritisieren die fehlende sichere Authentifizierung der Lichtbilder im derzeitigen Verfahren unter Berufung auf die Stellungnahme der EU-Kommission vom 24. Mai 2011 (s. Anlage).

Da der Beschlusstext und die zugrunde liegenden Argumente erst 2 Tage vor der Sitzung bei der Ärztekammer Nordrhein eingingen, stand aus Sicht der Vorsitzenden nicht ausreichend Zeit zur Verfügung, um den Sachverhalt zu prüfen und das Thema für die Sitzung aufzubereiten.

Frau Dr. Groß nimmt den Inhalt der Anträge als zur Identifikationsüberprüfung gehörendes – und damit sehr wichtiges Thema des ärztlichen Beirates – auf und bietet an, das Thema in der nächsten Sitzung des Beirates zu behandeln.

Herr Redders weist darauf hin, dass das BMG sowie die obersten Landessozialbehörden die Auffassung vertreten, dass § 291 SGB V keine Verpflichtung zur Identitätsüberprüfung bei der Lichtbildbeschaffung für die eGK enthält (s. Anlage). Herr Redders bietet außerdem an, weitere Fragen zum Thema gerne auch im bilateralen Gespräch zu klären.

### **TOP 6.3 Nächste Sitzung**

Die nächste Sitzung findet statt am 31.08.2011 in den Räumlichkeiten der Kassenärztlichen Vereinigung Westfalen-Lippe in Dortmund.

Themen der nächsten Sitzung:

- Lichtbildbeschaffungsprozess
- Zwischenbilanz und Ausrichtung der Arbeit des Ärztlichen Beirates