Abgeordnetenhaus BERLIN

Drucksache 17 / 14 468
Schriftliche Anfrage

17. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Prof. Dr. Niels Korte (CDU)

vom 02. September 2014 (Eingang beim Abgeordnetenhaus am 03. September 2014) und **Antwort**

Cloud-Computing in Berliner Krankenhäusern

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Vorbemerkungen: Die Schriftliche Anfrage trägt die Überschrift „Cloud-Computing in Berliner Krankenhäusern“. Es wird deshalb davon ausgegangen, dass die Fragestellungen sich aus-schließlich auf Berliner Krankenhäuser beziehen. Die Berliner Krankenhäuser sind gegenüber der für das Gesundheitswesen zuständigen Senatsverwaltung für Zwecke der Krankenhausplanung, der Investitionsplanung, der Krankenhausförderung und für weitere Maßnahmen zur Sicherstellung der Krankenhausversorgung (§ 26 des Landeskrankenhausgesetzes (LKG)) auskunftspflichtig. Im Hinblick auf darüber hinausgehende Informationen wie beispielsweise abgeschlossene privatrechtliche Verträge besteht gegenüber der für das Gesundheitswesen zuständigen Senatsverwaltung keine Auskunftspflicht. Die Beantwortung der Fragen durch die landeseigenen Krankenhäuser Charité und Vivantes sind im Folgenden gesondert gekennzeichnet.

1. Wie viele medizinische Einrichtungen in Berlin nutzen die Möglichkeit Daten im sog. Cloud-Computing zu speichern?

2. Welche Anbieter werden in Berlin für das Cloud-Computing genutzt und sind diese mindestens im Europäischen Wirtschaftsraum angesiedelt und beachten diese die europäischen Datenschutz-richtlinien?

Zu 1. und 2.: In Berlin wie auch weltweit bieten Dienstleister sowohl Behörden als auch Unternehmen verstärkt Cloud Computing an. Dem Senat liegen keine Erkenntnisse dazu vor, dass Berliner Krankenhäuser Angebote des Cloud Computing für die Verar-beitung von Patientendaten nutzen. Auf Anfrage teilte der Berliner Beauftragte für Datenschutz und Informationsfreiheit mit, dass auch ihm keine Verfahren von Berliner Krankenhäusern bekannt sind, im Rahmen derer eine Verarbeitung von Patientendaten durch einen Cloud-Service-Anbieter erfolgt. Vivantes: „Vivantes speichert keine Patientendaten in Cloud-Systemen, sondern speichert die Daten nur auf eigenen Systemen. Ein System wird ab dem 01.10.2014 extern im Rechenzentrum der Charité gehostet. Die Anbindung erfolgt nicht über öffentliche Netze. Die kompletten fachlichen Betriebs- und Betreiberleistungen liegen bei der Vivantes. In der gemeinsam mit der Charité betriebenen Tochtergesellschaft Labor Berlin wird das buchhalterische Einkaufssystem als Cloud-Lösung betrieben. In dem System werden keine Patientendaten verarbeitet. Insofern sind keine Datenschutzvorgaben zu berücksichtigen.“

Charité: „Die Charité speichert Daten ausschließlich intern bzw. hat eine eigene, sogenannte „Private Cloud“ aufgebaut, um den sicheren Austausch von Daten, nicht jedoch Patientendaten, auf Basis der datenschutzrechtlichen Vorgaben zu gewähr-leisten. Diese „Private Cloud“ steht voll unter der Kontrolle der Charité- Universitätsmedizin und stellt insofern eine sichere Alternative zu öffentlichen Cloud-Diensten dar. Die Charité nutzt keine externen Cloud-Anbieter. Stattdessen hat die Charité interne Möglichkeiten geschaffen und sieht sich eher als Service-Provider für die sichere Speicherung von Krankenhausdaten. Es ist geplant, weiteren externen Einrichtungen des Gesundheitswesens diesen Service aus der Charité gegen Vergütung sicher zur Verfügung zu stellen. In Vorbereitung befindet sich allerdings ein Online-Terminplanungssystem unter Nutzung eines externen Cloud-Anbieters. Patientinnen und Patienten hätten mit dem System u. a. die Möglichkeit, Termine in der Charité selbst zu buchen. Den Anforderungen des Datenschutzes und vor allem der Wahrung der ärztlichen Schweigepflicht wird durch den Einsatz eines patentierten kryptographischen Verfahrens entsprochen. Dieses Verschlüsselungsverfahren ermöglicht es ausschließlich der Nutzerin oder dem Nutzer und durch ihn Berechtigte die Daten einzusehen. Die Daten werden ausschließlich in kryptographischer Form über-mittelt und werden erst im Systembereich der Charité - Universitätsmedizin Berlin entschlüsselt dargestellt. Die Nutzung kann als optionaler, freiwilliger Service nur bei dokumentiertem Einverständnis des Patienten erfolgen.“

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

3. Wird überprüft, wo die Anbieter des Cloud-Computings sensible Patientendaten speichern und in welchen Ländern stehen die Datenserver?

Zu 3.: § 24 Absatz 7 Satz 1 LKG regelt für die Auftragsdatenverarbeitung, dass Patientendaten grundsätzlich nur im Krankenhaus oder im Auftrag durch ein anderes Krankenhaus verarbeitet werden dürfen. Durch andere Stellen dürfen Patientendaten im Auftrag des Krankenhauses nur verarbeitet werden, wenn durch technische Schutz-maßnahmen sichergestellt ist, dass der Auftragnehmer keine Möglichkeit hat, beim Zugriff auf Patientendaten den Personenbezug herzustellen (§ 24 Absatz 7 Satz 2 LKG). Ob sich das Cloud Computing für die Verarbeitung von Patientendaten unter Beachtung des § 24 Absatz 7 LKG überhaupt eignet, ist fraglich. So hat die Charité dazu ausgeführt, dass sie aufgrund der nicht immer klaren Länderzuordnungen entschieden habe, keine externen Cloud-Anbieter zur Speicherung von sensiblen medizinischen Patientendaten zu nutzen. Da dem Senat keine Erkenntnisse dazu vorliegen, dass Berliner Krankenhäuser Angebote des Cloud Computing für die Verarbeitung von Patientendaten nutzen, erübrigt sich die Beantwortung der Frage.

4. Welche Krankenhäuser benutzen kryptografische Verschlüsselungen und welcher Datenverschlüsselungsstandard wird genutzt?

Zu 4.: Die Arbeitskreise “Gesundheit und Soziales” und “Technik” der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe zu “Krankenhausinformationssystemen” erstellt. Der Senat geht davon aus, dass die Berliner Krankenhäuser weitgehend kryptographische Verschlüsselungen benutzen und die Berliner Krankenhäuser bemüht sind, entsprechende Empfehlungen der Orientierungshilfe Krankenhausinformationssysteme (2. Aufl.) umzusetzen.

Vivantes: „Für das bei der Charité gehostete System werden für die Datenspeicherung sogenannte selbstverschlüsselnde Plattensysteme eingesetzt. Diese erfüllen den FIPS 140-2 Standard. Es wird der AES 256 Verschlüsselungsalgorithmus verwendet. Das System ist direkt in das physikalische IT-Netzwerk der Vivantes integriert. Datenüber-tragungen über öffentliche Netze erfolgen nicht.“

Charité: „Klinische Daten werden in den internen Systemen nicht verschlüsselt gehalten. Allerdings bieten mittlerweile Speichersysteme hardwareseitige Verschlüsselungsmethoden. Die Charité plant, diese im nächsten Investitionszyklus einzuführen. Die Festplatten werden nach Einführung dieser Technik im Standard AES 256 mit FDE (Full Disk Encryption) verschlüsselt.“

5. Wer hat Zugang zu den Cloud-Daten und welchen Zugang haben die Anbieter zu den Cloud-Daten?

Zu 5.: Dem Senat liegen keine Erkenntnisse dazu vor, dass Berliner Krankenhäuser Angebote des Cloud Computing für die Verarbeitung von Patientendaten nutzen. Daher erübrigt sich die Beantwortung der Frage.

Vivantes: „Den Zugang zu dem in der Charité gehosteten System haben ausschließlich Vivantes-Mitarbeiterinnen und Vivantes-Mitarbeiter im Rahmen ihrer Dienstaufgaben über das geschlossene, sichere Vivantes-IT-Netz. Charité-IT-Mitarbeiterinnen und Charité-IT-Mitarbeiter haben Zugang zu dem System im Rahmen ihrer Rechenzentrumstätigkeiten.“

Charité: „Die interne Cloud wird ausschließlich von befugten Mitarbeiterinnen und Mitarbeitern der Charité genutzt, welche Externe zur Mitnutzung unter expliziter Beachtung der Nutzerrichtlinie autorisieren können. Als Anbieter haben ausschließlich autorisierte Mitarbeiterinnen und Mitarbeiter des Geschäftsbereichs IT der Charité vollen Zugriff auf die Daten.“

6. Inwieweit wird sichergestellt, dass die Verschlüsselung stets auf dem aktuellen Stand der Technik ist?

7. Überprüft der Senat die Vertragsgestaltung zwischen Krankenhäusern und Cloud-Anbietern auf die Einhaltung der Datenschutzbestimmungen? Gibt es einen Mustervertrag und wie sieht dieser aus?

Zu 6. und 7.: § 5 Absatz 1 Satz 2 des Berliner Datenschutzgesetzes (BlnDSG) schreibt vor, dass die Art und Weise der Maßnahmen für den angestrebten Schutzzweck angemessen zu sein hat und sich nach dem jeweiligen Stand der Technik richten muss. Die Einhaltung der datenschutzrechtlichen Vorgaben überprüft nicht der Senat, sondern der dafür zuständige Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Charité: „In der internen Cloud der Charité wird bisher keine Verschlüsselung eingesetzt. Der Einsatz mobiler Lösungen ist in Vorbereitung. Den höheren Risiken in der Nutzung mobiler Endgeräte soll u. a. durch die Verwendung kryptographischer Verfahren begegnet werden. Insofern ist auch der Einsatz von Verschlüsselungstechniken in Vorbereitung. Die Sicherstellung des technisch aktuellen Standes der eingesetzten Verschlüsselung wird organisatorisch durch regelmäßiges Verfolgen der einschlägigen Fachpublikationen, z. B. Mitteilungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), und der Herstellerinformationen gewährleistet. Werden Schwach-stellen der verwendeten Verschlüsselungstechnik bekannt, so erfolgt eine Anpassung auf den jeweils aktuellen Stand der Technik durch Updates oder ggf. durch einen Produktwechsel.“

Da dem Senat keine Erkenntnisse dazu vorliegen, dass Berliner Krankenhäuser Ange-bote des Cloud Computing für die Verarbeitung von Patientendaten nutzen, erübrigt sich die Beantwortung der Frage 7.

8. Werden die Patienten im Land Berlin über die Speicherung und Weitergabe ihrer Daten informiert und wie werden sie informiert? Erfolgt hierzu eine Einwilligung des Patienten? (§ 4a Abs. 1,3 BDSG)

9. Dürfen Patientendaten über die Cloud auf mobilen Endgeräten abgerufen werden und welche Richtlinien sind hierbei einzuhalten?

Zu 8. und 9.: Das Verarbeiten, Nutzen, Übermitteln und Offenbaren von Patientendaten ist nur zulässig, soweit dafür eine gesetzliche Grundlage existiert oder die Betroffenen eingewilligt haben (vgl. § 24 Absatz 3 LKG, § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG)). Soweit weder eine gesetzliche Grundlage noch eine Einwilligung vorliegt, ist die Datenvereinbarung von Patientendaten verboten und muss unterlassen werden. Einen anderen Sachverhalt betrifft der Hinweis auf die Datenverarbeitung. Aufgrund des § 4 Absatz 3 BDSG ist ein Krankenhaus verpflichtet, Patientinnen und Patienten bei Abschluss des Behandlungsvertrages davon in Kenntnis zu setzen, dass Daten über die Person, den sozialen Status sowie die für die Behandlung notwendigen medizinischen Informationen gespeichert, geändert bzw. gelöscht werden und im Rahmen der Zweckbestimmung unter Beachtung der jeweiligen datenschutzrechtlichen Regelungen an Dritte (z. B. Kostenträger) übermittelt werden. Für jedes Krankenhaus besteht damit die gesetzliche Verpflichtung, seine Patientinnen und Patienten über die Erhebung seiner Daten zu informieren. Soweit dies auf einer gesetzlichen Grundlage basiert, ist eine Einwilligung der Patientinnen und Patienten nicht erforderlich.

Vivantes: „Bei Vivantes erfolgt dies im Rahmen der Patientenaufnahme."

Charité: „Im Behandlungsvertrag werden die Patientinnen und Patienten über eine mögliche Weitergabe von Daten an Dritte, z. B. an die Labor Berlin GmbH, informiert. Werden z. B. Daten zum Zweck des privatärztlichen Honorarmanagements an Dritte weitergegeben, so erfolgt dies ausschließlich nach Information und Einwilligung der Patientinnen und Patienten. Die Einwilligung wird mit Unterschrift dokumentiert und der Patientin oder dem Patienten bleibt die Option einer Ablehnung."

Da dem Senat keine Erkenntnisse dazu vorliegen, dass Berliner Krankenhäuser Angebote des Cloud Computing für die Verarbeitung von Patientendaten nutzen, erübrigt sich die Beantwortung der Frage 9.

Vivantes: „Für das bei der Charité gehostete System ist ein Datenabruf über mobile Geräte nicht möglich."

Charité: "Aktuell werden keine Patientendaten auf mobilen Endgeräten über die Cloud abgerufen. Künftig soll dies ermöglicht werden. Dies insbesondere dann, wenn Leib und Leben der Patientinnen und Patienten geschützt werden können. Die Kommunikation zwischen den mobilen Endgeräten und den datenführenden Systemen wird mit einer Ende-zu-Ende-Verschlüsselung gesichert werden. Die Richtlinie für die Nutzung mobiler Endgeräte in diesem Szenario ist bereits erstellt und definiert präzise den Zweck sowie den Einsatzort und berücksichtigt alle vom Bundesamt für Sicherheit in der Informationtechnik (BSI) definierten Empfehlungen für mobile Arbeitsplätze. Jede Nutzerin oder jeder Nutzer wird gesondert auf die spezifischen Risiken in der Nutzung mobiler Endgeräte hingewiesen. Die Kenntnisnahme und das Verständnis der in einer Dienstanweisung und gesonderten Belehrung zusammen-gefassten Risiken wird in einem Übergabeprotokoll durch Unterschrift dokumentiert."

10. Wie wird die Nutzung von Patientendaten auf externen Servern, die von Drittanbietern zur Verfügung gestellt werden, auf eine Vereinbarkeit mit § 203 StGB, § 3-5, 11 BDSG und § 24, 25 LKG Berlin und anderen einschlägigen Rechtsvorschriften geprüft?

Zu 10.: Krankenhäuser sind gesetzlich verpflichtet, die datenschutzrechtlichen Bestimmungen einzuhalten und das Patientengeheimnis zu wahren. Soweit überhaupt die Nutzung von Patientendaten auf externen Servern in Frage kommt, ist es Aufgabe des krankenhausinternen Datenschutzbeauftragten (§ 4 f Absatz 1 BDSG), die Vereinbarkeit mit den relevanten datenschutzrechtlichen Vorschriften zu prüfen (vgl. § 4 g BDSG). Nach den standesrechtlichen bzw. strafrechtlichen Regelungen ist die Ärztliche Direktorin oder der Ärztliche Direktor bzw. die Ärztliche Leiterin oder der Ärztliche Leiter für die Wahrung des Patientengeheimnisses verantwortlich und verpflichtet, die Ein-haltung der ärztlichen Schweigepflicht zu überwachen.

Vivantes: „Für das in der Charité gehostete System wurden die entsprechenden Prüfungen durch den betrieblichen Datenschutzbeauftragten vorgenommen und die entsprechenden Auftragsdatenverarbeitungsverträge nach § 11 BDSG inklusive der technischen und organisatorischen Beschreibungen abgeschlossen."

Charité: „Eine Verarbeitung von Patientendaten auf externen Servern erfolgt nicht. (Sollten Patientendaten auf externen Servern verarbeitet werden, so wäre ein Vertrag zur Auftragsdatenverarbeitung gemäß § 11 BDSG, § 3 BlnDSG zu schließen. Die TOM (technische und organisatorische Maßnahmen) gemäß § 9 BDSG, § 5 BlnDSG regeln insbesondere die Zugangs-, Zutritts- und Zugriffskontrolle. Die Vereinbarkeit mit § 203 Strafgesetzbuch (StGB) könnte dabei nur gewährleistet werden, wenn die Daten ausschließlich in kryptographischer, anonymisierter oder pseudonymisierter Form übermittelt und erst im Systembereich der Charité - Universitätsmedizin Berlin entschlüsselt dargestellt würden)."

11. Welche Maßnahmen plant der Senat im Bereich des Cloud-Computings in landeseigenen Krankenhäusern?

Zu 11.: In Teil 1 der Orientierungshilfe zu "Krankenhausinformationssystemen" (vgl. Antwort zu Frage 4.) sind die Anforderungen konkretisiert, die sich aus den geltenden datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Kranken-häusern ergeben. Damit liegt für die Hersteller von Krankenhausinformationssystemen, die Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor. Nach den Erkenntnissen des Senats wird die Orientierungshilfe nicht nur in den landeseigenen sondern auch in den übrigen Krankenhäusern zunehmend berücksichtigt. Darüber hinausgehende Maßnahmen plant der Senat nicht.

Charité: „Die Charité - Universitätsmedizin Berlin möchte sich als Anbieter einer „Medical-Cloud" für die Region Berlin und Brandenburg etablieren. Kleineren Gesundheitseinrichtungen kann so die rechtssichere Nutzung moderner IT-Verfahren ermöglicht werden.

So könnte die Charité - Universitätsmedizin Berlin beispielsweise ein IHE-konformes Archiv anbieten, welches die zu archivierenden Daten beweiswerterzeugend und beweiswerterhaltend speichert."

Berlin, den 23. September 2014

In Vertretung

Emine D e m i r b ü k e n - W e g n e r

Senatsverwaltung für
Gesundheit und Soziales

(Eingang beim Abgeordnetenhaus am 24. Sep. 2014)