EHEALTHCOM
Magazin für Health-IT, vernetzte Medizintechnik und Telemedizin

Bring your own device - private Smartphones im Krankenhaus Haftungsrisiken und –prävention

Rechtsanwalt Dr. iur. Oliver Pramann, Kanzlei 34 Rechtsanwälte und Notare, Königstraße 34, 30175 Hannover

cand. iur. Barbara Garz, Mühlenweg 12a, 29356 Bröckel

Dr. med. Urs-Vito Albrecht, MPH, PLRI MedAppLab, P.L.Reichertz Institut für Medizinische Informatik der Medizinischen Hochschule Hannover, Carl-Neuberg-Straße 1, 30625 Hannover

Das Angebot an mobilen Endgeräten wie Smartphones oder Tablet-PCs ist riesig und nimmt immer weiter zu. Das gleiche gilt für Applikationen (Apps), die gemeinsam mit den mobilen Geräten den aktuellen Lifestyle prägen. Fast jeder Arbeitnehmer im Krankenhaus besitzt ein oder mehrere mobile Endgeräte, die er mit für ihn hilfreichen Apps ausgestattet hat. Apps sind für nahezu jedes Anwendungsfeld denkbar, so auch für den medizinischen Bereich. Dass gerade auch hier eine zunehmende Tendenz zu bemerken ist, zeigt eine Untersuchung des Branchenverbands BITKOM, der aktuell ca. 15.000 Apps in der Rubrik “Medizin” zählt.[1] Parallel zu dieser Entwicklung kann in Unternehmen das Phänomen Bring your own device (BYOD) beobachtet werden. Arbeitnehmer bringen ihr privates mobiles Endgerät mit in den Betrieb und nutzen dies - vom Arbeitgeber geduldet oder nicht geduldet - für betriebliche Zwecke.

Unabhängig davon, ob der Arbeitgeber die Nutzung von privaten mobilen Geräten für betriebliche Zwecke respektive die Nutzung von betrieblichen mobilen Geräten für private Zwecke akzeptiert, drohen durch die Verquickung der Anwendungsbereiche Gefahren für die Sicherheit des hauseigenen Datennetzes. Daneben können sich rechtliche Fallstricke, angefangen von arbeitsrechtlichen Problemen des Arbeitnehmers bis hin zu urheber- und lizenzrechtlichen Problemen des Arbeitgebers ergeben. Konkret sind im Wesentlichen datenschutzrechtliche, arbeitsrechtliche und auch strafrechtliche Rechtsbereiche tangiert, wobei jeweils präventiv seitens des Arbeitgebers entsprechendes Tätigwerden angezeigt ist.
Als eine adäquate Maßnahme zum Schutz des Krankenhauses ist die Gestaltung und Umsetzung einer hauseigenen IT-Richtlinie, welche die Sicherheitsbestimmungen und den Umgang mit mobilen Geräten festlegt. Grundlage hierfür können die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der Richtlinie „mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdung und Schutzmaßnahmen“ sein. Die Richtlinie sollte den hausinternen Besonderheiten angepasst und dem jeweils aktuellen Stand der Technik angepasst werden, da die BSI-Empfehlung aus dem Jahr 2006 stammt und Besonderheiten individueller Krankenhäuser nicht darstellen kann.

Der vorliegende Beitrag will ausgehend von dem tatsächlichem Phänomen BYOD die Gefahren für das hausinterne Netz sowie die rechtlichen Berührungspunkte und die damit verbundenen Haftungsprobleme aufzeigen. Weiter sollen auf der Grundlage der Empfehlungen des BSI Eckpunkte für eine mögliche hausinterne IT-Richtlinie vorgestellt werden.

1. Einsatz privater mobiler Endgeräte am Arbeitsplatz

Die Anwendungsfelder mobiler Endgeräte und Apps reichen weit über das private Umfeld hinaus. Gerade im medizinischen Umfeld werden unterschiedlichste Apps für Ärzte und/oder Patienten angeboten. Als Medical-App im Krankenhausbereich kommt Software mit dem Zweck „mobile Visite mit Datenerfassung am Krankenbett, Zugriff auf Daten aus dem Krankenhausinformationssystem, diktieren von Arztbriefen mit digitaler Spracherkennung, OP-Plan-Ansicht, Terminplan für Patienten, Medikamenten-Datenbanken, Anforderungen und Auftragserteilungen, Dokumentation, automatisierte Auswertung von Vitalparametern oder Patienteninformationen“ in Betracht.[2]

Da die Anwendung der mobilen Geräte und den hilfreichen Apps die Praxis durchaus erleichtern kann, ist damit zu rechnen, dass der professionelle Einsatz zunimmt. Mit diesem Phämomen sollte sich das Krankenhaus, auch in seiner Funktion als Arbeitgeber und Verantwortlicher gegenüber den Patienten auseinandersetzen.

Beachtenswert ist, dass Apps existieren, die als Medizinprodukte nach dem Medizinproduktegesetz vermarktet werden, da sie aufgrund ihrer medizinischen Zweckbestimmung durch den Hersteller Medizinprodukt in Gestalt einer Stand-alone-Software sind. Diese Software hat dann zwangsläufig ein sogenanntes Konformitätsbewertungsverfahren auf der Grundlage des Medizinproduktegesetzes und der Medical Device Directive (MDD) durchlaufen und bietet so durch die CE-Kennzeichnung einen Nachweis für entsprechende Sicherheit.[3] Die überwältigende Mehrheit der medizinischen Apps kann jedoch einen solchen Nachweis nicht erbringen, da sie entweder tatsächlich kein Medizinprodukt sind oder vom Hersteller zu Unrecht nicht als solches eingestuft wurden. Für die Anwender und damit auch für die Verantwortlichen - wie den Krankenhausträger - bedeutet das, dass sich bei professionellem Einsatz der Apps eine Haftungsfalle eröffnen kann.[4]

Die praktische Anwendung von mobilen Geräten im Krankenhaus ergibt ein weiteres Problem, welches insbesondere mit dem Einsatz im Kontakt mit den Patienten zusammenhängt. Der Handkontakt in der Anwendung von Touchscreens kann eine Kontamination und Verbreitung von Krankheitserregern zur Folge haben. Nur durch Sicherstellung einer hinreichende Desinfektion kann dies und somit eine mögliche Haftungfalle vermieden werden.[5]

2. Gefahren für das hausinterne Datennetz

Beim Einsatz privater Geräte mit Anschluss an das hausinterne Datennetz kann sich ein erheblicher Unsicherheitsfaktor ergeben. Viren, Würmer, Trojaner und Backdoors können eingeschleust werden. Auch die Geräte selbst können durch Angriffe auf die Hardware manipuliert oder zerstört werden. Informationen auf dem Gerät könnten gestohlen oder Nutzungsspuren durch die Installation entsprechender Software ausspioniert werden.

Sobald Dritte Zugriff auf Betriebssysteme und Dienste erlangen, können diese durch Systemtests, konkrete Analysen, Versionsstände und Art der Software, Rückschlüsse auf die Sicherheitspolicy des Unternehmens ziehen. Wenn die Schwachstellen des Systems eruiert werden, können sich die Angriffe nicht nur auf das analysierte Endgerät, sondern Angriffe auf

alle Geräte mit gleicher Policy vorgenommen werden. Viren, Würmer und Trojaner könnten eingebracht, Gegenmaßnahmen ausgehebelt oder Passwörter ausspioniert werden. Bei Anwendungen könnten Authentisierungsprüfungen umgangen, Programmierfehler ausgenutzt oder Logging- und Accountingdaten verändert werden.

Angriffe auf die Infrastruktur würden sich durch Einschleusung von Schadsoftware, Einsatz manipulierter oder fremder mobiler Geräte, Diebstahl vertraulicher Informationen, Unerlaubte Dienstnutzung, illegalen Datentransport großer Datenmengen, Rechtemissbrauch (in der Infrastruktur des Hauses) oder Manipulation von Netzwerkkomponenten und Arbeitsplatzsystemen äußern. Gefahren können sich auch aus der Analyse und dem Ausnutzen des Administrationskonzepts, der Beeinflussung des Update- und Konfigurationsmanagements ergeben.[6]

Auch im Bereich der Kommunikation sind Angriffe möglich: Synchronisation, Missbrauch des Servicebusses oder Spoofing-Angriffe durch Vortäuschung falscher Identitäten, Beobachtung der Kommunikation durch Sniffing-Angriffe und Aufzeichnung von Bewegungsprofilen sind dadurch möglich.

3. Präventive Maßnahmen zum Schutz des Krankenhausnetzes

Das Krankenhaus sollte sich den oben genannten Gefahren für das Unternehmen zunächst bewusst werden. Da die Gefahren aus dem Einsatz der privaten mobilen Geräte am Arbeitsplatz resultieren, muss die Prävention an dieser Stelle beginnen. Durch eine entsprechende hausinterne IT-Richtlinie zur Gewährleistung der Sicherheit kann das Krankenhaus einen wichtigen Schritt zum Schutz des Netzes und der verarbeiteten sensiblen Daten gehen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in der Richtlinie „mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdung und Schutzmaßnahmen“ aus dem Jahr 2006 Probleme und Lösungsvorschläge zur Gestaltung und Umsetzung einer IT-Sicherheitsrichtlinie veröffentlicht, die als Grundlage einer individuellen hausinternen Sicherheitsrichtlinie dienen kann.[7] So wurde diese Richtlinie bereits für aktuelle Richtlinien verwendet und an den aktuellen Stand der Technik angepasst.

Der Ansatz beginnt beispielsweise schon beim Kauf der Geräte. Schon bei der Auswahl und er Beschaffung sollte darauf geachtet werden, dass sich die Geräte ohne wesentliche Veränderungen einpassen lassen. Die Bezugsquelle der Geräte und der Hersteller müssen vertrauenswürdig sein (Hardwarehersteller und Provider können Software auf das Gerät bringen) und die bereits im Gerät vorhandenen Sicherheitsmechanismen müssen entsprechenden Schutz gewährleisten.

In den Empfehlungen des BSI finden sich ferner Eckpunkte. Einer hat einen Leitfaden zur Erstellung einer Sicherheitsrichtlinie mit Regeln und den Anforderungen an die Einsatzumgebung. Diese wurden bereits von Krankenhäusern als Grundlage einer hauseigenen Sicherheitsrichtlinie unter Beachtung des aktuellen Stands der Technik verwendet, da die Empfehlungen des BSI aus dem Jahr 2006 stammen.[8] Folgende Punkte können, freilich ohne Anspruch auf Vollständigkeit, wichtige Eckpunkte einer solchen Richtlinie bilden.

a. physische Sicherung

- Schutz vor direktem Zugriff Dritter
- Schutz gegen Diebstahl des Geräts
- Verbot der Weitergabe des Mobilgeräts an Dritte außerhalb des Krankenhauses
- Pflicht der Anzeige im Krankenhaus bei Verlusts

b. Schutz der Daten auf dem Gerät

- Aktivierung von Kennwortschutz
- automatische passwortgeschützte Sperrung bei Inaktivität
- Vermeidung und ggf. Verschlüsselung der Speicherung von personal- und patientenbezogenen Daten
- Speicherung von personal- und patientenbezogenen Daten auf externen Datenträgern nur mit einer Verschlüsselung nach dem aktuellen Stand der Technik
- “Cloud-Computing” nur mit Genehmigung
- Untersagung der Installation von Anwendungen, die das Recht fordern, auf die Kontaktlisten lesend und schreibend zuzugreifen
- Keine lokale Speicherung von Passwörtern

c. Schutz vor Angriffen auf die Kommunikation

- Deaktivierung von WLAN, Bluetooth, Infrarot- und anderen Kommunikationsschnittstellen, wenn diese nicht gerade aktiv benutzt werden
- Keine Speicherung von personal- und patientenbezogenen “in der Cloud”
- Verbot der Umgehung des Krankenhausnetzes
- Datenübertragung nach Möglichkeit nur über verschlüsselte Kanäle

d. Außerbetriebnahme

- Sicherung der auf dem Gerät gespeicherten Daten
- unwiederbringliche Löschung der Daten auf dem Gerät
- Zurücksetzung der Konfiguration

4. Rechtliche Risiken

Aus den oben genannten technischen Risikofeldern des Einsatzes privater mobiler Endgeräte im klinischen Setting ergeben sich auch rechtliche Risiken die bereits außerhalb des speziellen Anwendungsfeld "Krankenhaus" zum Themenkomplex BYOD diskutiert werden. Im Krankenhaus sind sie aufgrund des besonders sensiblen Bereichs von sehr großer Bedeutung. Die Problemkreise ranken u.a. um Arbeitsrecht, Urheberrecht und Datenschutzrecht. Bei der Betrachtung ist zu konstatieren, dass eine große Anzahl von Arbeitnehmern ihre privaten mobilen Endgeräte tatsächlich auch zu betrieblichen Zwecken einsetzt.

Ein erster Gesichtpunkt ist die auf dem privaten Gerät installierte Software. Das Nutzungsrecht hat hier zunächst nur der Arbeitnehmer erworben. Die Einräumung einer Nutzungsmöglichkeit für den Arbeitgeber würde eine unzulässige Übertragung darstellen. Das bedeutet, dass der Arbeitgeber zusätzlich Lizenzen erwerben müsste.[9] Eine Nutzung des Arbeitgebers ist sonst grundsätzlich nicht zulässig.

a. Verhältnis Arbeitgeber und Arbeitnehmer

Im Verhältnis zwischen Arbeitnehmer und Arbeitgeber können ebenfalls verschiedene rechtliche Problemfelder auftreten, die mit der Nutzung privater Geräte am Arbeitsplatz zusammenhängen. Kann der Arbeitgeber von seinen Arbeitnehmern verlangen, seine privaten Geräte zu betrieblichen Zwecken einzusetzen? Im Ergebnis nicht. Grundsätzlich ist

es nicht die arbeitsvertragliche Pflicht des Arbeitnehmers, private Endgeräte anzuschaffen und zu betrieblichen Zwecken einzusetzen. Der Arbeitgeber muss dafür Sorge tragen, dass er die notwendigen Ressourcen für die Arbeitnehmer zur Verfügung stellt. Weder aus dem rechtlichen Konstrukt eines sog. Gefälligkeitsverhältnisses bei dem die Nutzung nur gelegentlich und unentgeltlich erfolgt oder einer Leihe im Sinne einer zeitweisen unentgeltlichen Überlassung der Geräte vom Arbeitnehmer an den Arbeitgeber, kann ein Rechtsanspruch des Arbeitgebers begründet werden. Allenfalls durch eine betriebliche Übung, d. h. eine Verfestigung der Praxis, Betriebsaufgaben mit mobilen Endgeräten der Mitarbeiter zu erledigen, kann sich ein Anspruch begründen. Hierfür müsste jedoch der Arbeitnehmer schlüssig durch sein Verhalten eine Zustimmung zur betrieblichen Nutzung geben, auf die der Arbeitgeber vertrauen darf. Ob ein solcher Fall vorliegt, ist allerdings immer im Einzelfall zu prüfen.[11]

Wenn der Arbeitgeber für den Arbeitnehmer die Wartung bzw. eventuelle Reparaturen des Gerätes übernehmen soll, kann eine Pflicht für den Arbeitgeber hierzu nur durch gesonderte Vereinbarung geschaffen werden. Üblicherweise obliegt es dem Eigentümer des Gerätes, für die Wartung und Reparatur des Gerätes zu sorgen. Umgekehrt würde auch der Arbeitnehmer nur durch eine explizite Verpflichtung hierzu in die Pflicht genommen werden können. Entsprechendes gilt bei Verlust oder Defekt. Hier ist der Arbeitnehmer nicht verpflichtet, ein neues zu beschaffen, wenn keine vertragliche Regelung dazu existiert. Sind jedoch die Schäden oder der Verlust vom Arbeitgeber zu vertreten, so ist er zur Reparatur bzw. zur Neubeschaffung verpflichtet. Unter Umständen kann es zu einer Haftung des Arbeitnehmers kommen, wenn er absichtlich oder aus Fahrlässigkeit betriebliche Daten auf seinem mobilen Endgerät löscht.[12]

b. Datenschutz

Ein datenschutzrechtliches Problem kann sich immer dann ergeben, wenn der Arbeitnehmer im Zuge der Nutzung seines Gerätes auf die Daten des Arbeitgebers zugreift, wo personenbezogene Daten von beispielsweise Kunden oder Patienten verarbeitet werden. Der Arbeitgeber muss sicherstellen, dass dieser Zugriff zur Nutzung nicht zu weit reicht. Zur Absicherung muss der Arbeitgeber die Daten kontrollieren und überwachen, die sich auf die betriebliche Arbeit beziehen.

Das Bundesdatenschutzgesetz (BDSG) findet für nicht öffentliche Stellen immer dann Anwendung, wenn personenbezogene Daten erhoben, verarbeitet und genutzt werden, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten. Es ergeben sich mithin Kontrollpflichten für den Arbeitgeber, die mit dem Zugriff des Arbeitnehmers auf das private Gerät einhergehen. Zur Vermeidung einer Verletzung von Persönlichkeitsrechten der Arbeitnehmer sollten solche Kontrollen daher vertraglich vereinbart werden. Die Kontrollen selbst sollten auf das notwendigste Maß und auf dienstliche Daten beschränkt werden, soweit dies möglich ist.

Steht das mobile Endgerät im Eigentum des Arbeitgebers, stellen sich die dargestellten Probleme nicht in dieser Weise, da es dem Arbeitgeber möglich ist, vertraglich zu vereinbaren, dass die Geräte ausschließlich für betriebliche Zwecke genutzt werden.[13]

c. Urheberrecht

Problematisch können Urheberrechtsverstöße von Arbeitnehmern sein, für die der Arbeitgeber unter Umständen gegenüber dem dem Inhaber der Rechtehaften muss. Unterlassung, Vernichtung, Rückruf oder Überlassung von rechtswidrig hergestellten Vervielfältigungsstücken sind mögliche Ansprüche nach dem Urhebergesetz (UrhG). Der Unternehmensinhaber kann auch dann haften, wenn der Arbeitnehmer die

Rechtsgutsverletzung ohne sein Wissen oder gegen seinen Willen begangen wurde[14], wobei der Arbeitnehmer die Rechtsgutsverletzung allerdings im Rahmen seiner Tätigkeit begangen haben muss**.**

Ein weiteres Problem kann sich durch illegale Software auf dem privaten Gerät ergeben. Es ergibt sich die Frage, ob sich der Arbeitgeber dies zurechnen lassen muss. Die Gestattung der Nutzung eigener Geräte spricht für eine Zurechnung. Dagegen spricht die fehlende Zugriffsmöglichkeit durch den Arbeitgeber, weil das Gerät im Eigentum des Arbeitnehmers steht.[15] Eine Zurechnung soll immer dann ausscheiden, wenn die Handlung allein dem Handelnden und nicht dem Unternehmen zugute kommt.[16]

Der Arbeitgeber kann dieses Zurechnungsproblem durch eine Vereinbarung mit den Mitarbeitern umgehen, worin die Möglichkeit der Prüfung des Geräts durch den Arbeitgeber verabredet wird. Den Arbeitnehmern sollten grundsätzlich verbindliche betriebsinterne Regelungen vorgegeben werden, wie die privaten Geräte im Rahmen der betrieblichen Nutzung genutzt werden können und dürfen. Diese können dann durch gelegentliche Kontrollen überprüft werden.[17]

5. Fazit

Auch im Krankenhaus werden private mobile Endgeräte der Arbeitnehmer auch zu betrieblichen Zwecken eingesetzt. Hiermit sind für die Beteiligten, insbesondere für das Krankenhaus als Arbeitgeber, eine große Anzahl von Risiken verbunden. Die Gefahren drohen in erster Linie dem Datennetz des Krankenhauses, wenn die Geräte eingebunden werden. Daneben existieren rechtliche Unsicherheiten u.a. im Arbeits-, Datenschutz- oder Urheberrecht.

Damit das Krankenhaus diesen Unsicherheiten begegnen kann, bieten sich entsprechende hausinterne IT-Richtlinien an, welche die Sicherheit im Umgang mit mobilen Endgeräten sicherstellen. Hierbei kann die Richtlinie des Bundesamt für Sicherheit in der Informationstechnik (BSI) Richtlinie „mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdung und Schutzmaßnahmen“ aus dem Jahr 2006 als Grundlage dienen, wenn sie den hausinternen Besonderheiten und dem aktuellen Stand der Technik angepasst wird.

Literatur

[1] BITKOM, Das Handy als Thermometer, Blutdruck- und Blutzuckermesser, http://www.bitkom.org/de/presse/70864_70347.aspx.

[2] Krüger-Brand HE: Smartphones und Tablet-PCs im Gesundheitswesen:Strategien für mobile Anwendungen. Dtsch Arztebl 2011; 108(45): [8].

[3] Gärtner A.: Mobilgeräte und Apps in der Medizin aus regulatorischer Sicht, http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/Gaertner_Mobilgeraete_und_Apps_aus_regulatorischer_ Sicht.pdf (Stand: 31.07.2012).

[4] Pramann, O in: Medizintechnik und Informatioinstechnologie, Mobile Endgeräte und medizinische Software-Applikationen im Krankenhaus, 07801, S. 9.

[5] O. Pramann, K. Graf, U.-V. Albrecht. Tablet-PC im Krankenhaus: Hygienische Aspekte beachten. Dtsch Arztebl 2012; 109(14): A 706–7.

[6] umfassend zu den Risiken und zur Prävention: Bundesamt für Sicherheit in der Informationstechnik: Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/MobilEndgeraete/mobile_endgeraete_pdf.pdf;jsessionid=F6202689484020D3187F49BB97BEC9E6.2_cid244?__blob=publicationFile (Stand: 31.07.2012).

[7] Bundesamt für Sicherheit in der Informationstechnik: Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahme, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/MobilEndgeraete/mobile_endgeraete_pdf.pdf;jsessionid=F6202689484020D3187F49BB97BEC9E6.2_cid244?__blob=publicationFile (Stand: 10.03.2013).

[8] Albrecht U.-V., Weiß R. G., Pramann O., Dienstliche Nutzung privater Geräte, Dtsch Arztebl 2012; 109(31/32): A 1545–6; Albrecht, U-V; Pramann, O; Jahn, U v, Medical-Apps: App-gehört – Datenschutzrisiken, Dtsch Arztebl 2012; 109(44): A-2213 / B-1805 / C-1769

[9] Schneider, ZD 2011, 153, 158; Koch, ITRB 2/2012 S. 35, 36.

[10] Koch, ITRB 2/2012 S. 35, 37.

[11] Koch, ITRB 2/2012 S. 35, 38.

[12] Schneider, ZD 2011, 153, 155; Tschol, IT business 1/2012 S. 2, 3.

[13] BGH, GRUR 2003, 453-454; BGH NJW 1992, 1310, 1311.

[14] Müller, ITRB 1/2012, S. 15, 16.

[15] BGH, GRUR 2007, 877-881.

[16] Müller, ITRB 1/2012, S. 15, 17.; Schneider, ZD 2011, 153, 156.