Universitätsklinikum Magdeburg A.ö.R.

Dienstvereinbarung (DV) 3/2018
zum Einsatz von Mobiltelefonen (Smartphones)
in der Universitätsmedizin Magdeburg

Zwischen

dem Universitätsklinikum Magdeburg A.ö.R.
vertreten durch den Klinikumsvorstand

und

dem Personalrat des Universitätsklinikums Magdeburg A.ö.R.
vertreten durch den Personalratsvorsitzenden

wird in Anwendung des § 70 Abs. 1 Personalvertretungsgesetz Land Sachsen-Anhalt (PersVG LSA) die nachfolgende Dienstvereinbarung (DV) geschlossen:

Grundsätzliche Regelungen

1. Sprachliche Gleichstellung

[1]Zum besseren Verständnis wird auf die Verwendung der weiblichen und männlichen Form verzichtet. [2]Alle Bezeichnungen gelten sowohl für weibliche als auch männliche Beschäftigte.

2. Persönlicher Geltungsbereich

Die Dienstvereinbarung gilt für alle Beschäftigten des Universitätsklinikums Magdeburg A.ö.R. auf die das Personalvertretungsgesetz des Landes Sachsen-Anhalt (PersVG LSA) Anwendung findet.

3. Sachlicher Geltungsbereich

(1) Diese Dienstvereinbarung regelt insbesondere den Umgang mit dienstlichen Smartphones, deren Verwendung zur Verbesserung der Verwaltungs- und Kommunikations-Prozesse von Klinikum und Fakultät ausgeweitet werden soll.

(2) Die Verwendung privater Mobiltelefone für dienstliche Belange wird in Anlage 4 beschrieben.

4. Allgemeines

[1]Leistungsfähige Smartphones haben auch für die mobile Unternehmenskommunikation eine zunehmende Bedeutung, die weit über die Funktion als mobiles Telefon hinausgeht. [2]Sie können aber auf Grund ihres Funktionsumfangs, ihrer Leistungsfähigkeit und permanenten Internet-Verbindung ein erhebliches Sicherheitsrisiko darstellen. [3]Deshalb sind für unternehmenskritische Anwendungen im Klinikums-Umfeld besondere Sicherheits-Maßnahmen erforderlich. Voraussetzung für eine sichere mobile Unternehmens-Kommunikation ist die Einbindung der Geräte in eine sichere Infrastruktur zur Mobilgeräte-Verwaltung und Anbindung an das Klinikums-Intranet.

5. Begriffsbestimmungen

(1) [1]Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. [2]Soweit für die Datenverarbeitung innerhalb der Telekommunikationsanlage zwischen Stamm-, Verbindungs-, Betriebs-, Gebühren- und Inhaltsdaten unterschieden wird, sind darunter im Einzelnen folgende Daten zu verstehen:
[3]Stammdaten sind personenbezogene Daten, die das Nutzungsverhältnis der jeweiligen Teilnehmerinnen und Teilnehmer festlegen oder aus anderen Gründen dauernd gespeichert sind.
[4]Verbindungsdaten sind gerätebezogene Daten, die zur Bereitstellung der Verbindung erforderlich sind: Rufnummern der anrufenden und angerufenen Geräte, Beginn und Ende der jeweiligen Verbindung, genutzte Leistungsmerkmale.
[5]Betriebsdaten sind gerätebezogene Daten, die zum Zwecke der Störungs-eingrenzung und -beseitigung sowie zur Verkehrsmessung zum Teil statistisch erhoben werden.
[6]Gebührendaten sind kostenstellenbezogene Daten, die zur Gebührenermittlung und Abrechnung zugelassen sind.
[7]Inhaltsdaten sind personenbezogene Daten über den Inhalt von Telefongesprächen oder Datenübermittlungen.

(2) Betreiberin der Mobilfunktelefone ist das Universitätsklinikum Magdeburg A.ö.R.

(3) Teilnehmer/Teilnehmerinnen bzw. Nutzer sind natürliche Personen, denen ein betriebliches Mobilfunktelefon zugeordnet wurde.

(4) Leistungsmerkmale sind technisch nutzbare Eigenschaften der Mobilfunkanlage für Teilnehmer, Teilnehmerinnen.

(5) [1]Als installiert werden Programme und Dateien bezeichnet, die vorhanden sind und vor der Benutzung nicht erst von externen Speichermedien eingespielt werden müssen. [2]Als installiert werden Leistungsmerkmale bezeichnet, wenn die für sie benötigten Programme und Dateien installiert sind und sie im Rahmen der Betriebsführung ohne das Einspielen zusätzlicher Software verfügbar sind.

(6) [1]Systemverwaltung ist die Summe der notwendigen Tätigkeiten zur Gebührendaten-erfassung, zur Eingabe, Verarbeitung und Ausgabe von Stammdaten und zur Verkehrsmessung. [2]Wartung bezeichnet die Tätigkeiten, die zur Aufrechterhaltung der Funktionsfähigkeit der Mobilfunktelefone erforderlich sind.

(7) Betriebsführung bezeichnet alle Tätigkeiten zur Systemverwaltung, -wartung und -erweiterung.

(8) Server sind Baugruppen bzw. Anlagen, die geeignet sind für Betriebsführung und Datenübertragung von und zur Vermittlungseinheit, sowie zur Speicherung von Text- und Fax-Nachrichten.

(9) Systemschnittstellen sind nicht teilnehmerbezogene Schnittstellen der Mobilfunktelefone, die geeignet sind zur Übertragung von Stamm-, Verbindungs-, Betriebs-, Gebühren- oder Inhaltsdaten.

(10) [1]Gebührendatenerfassung ist die Aufzeichnung der für die Gebührendaten-verarbeitung notwendigen Verbindungsdaten auf Datenträgern der Telekommunikationsanlage. [2]Gebührendatenverarbeitung ist die Berechnung der Gebühren auf Grund der aufgezeichneten Verbindungsdaten sowie die Erstellung und der Ausdruck der Gebührennachweise.

(11) Eine Sprach-Mail-Box ist ein elektronischer Anrufbeantworter auf dessen Inhalt ausschließlich der Endgerätenutzer und im Bedarfsfall seine Vertreterin/sein Vertreter Zugriff hat.

Prinzipielles technisches Sicherungskonzept

(1) [1]Mit Hilfe eines durch das Medizinische Rechenzentrum (MRZ) bereitgestellten universellen Mobile-Device-Management-Systems werden alle Mobilgeräte mit dienstlicher Nutzung zentral verwaltet, unabhängig vom Nutzungsprofil, von Geräte-Hardware und Betriebssystem. [2]Die Datenübertragung zwischen Mobilgerät und Klinikums-Intranet sowie die Daten-Speicherung auf den Geräten erfolgt verschlüsselt, Sicherheitsrichtlinien werden automatisch verteilt und überwacht. [3]Mit Hilfe abgesicherter Container-Apps werden dienstliche Daten auf den Mobilfunktelefonen sicher von den zum Betrieb der Mobilfunktelefone notwendigen Systemdaten und auf dem Gerät gespeicherten persönlichen Daten und Applikationen (Apps) getrennt. [4]Die im Smartphone verschlüsselt gespeicherten Unternehmensdaten können bei Verlust des Mobiltelefons zentral gelöscht werden.

(2)[1]Die technischen Angaben zu den Servern, den zum Einsatz kommenden Endgeräten sowie der verwendeten Software und ihrer Leistungsmerkmale sind in der Anlage 1 dieser Dienstvereinbarung zusammengefasst. [2]Diese Anlage wird jährlich aktualisiert.

Nutzerkreis

Zur Verbesserung der Verwaltungsprozesse und mobilen Erreichbarkeit der Leitungsebenen von Klinikum und Fakultät kann schrittweise - unter dem Vorbehalt der Finanzierbarkeit - der folgende Mitarbeiterkreis mit dienstlichen Smartphones ausgestattet werden:

1) Vorstände, Klinik- und Institutsdirektoren
2) Oberärzte und Leiter von Funktionsbereichen
3) Leiter der Geschäftsbereiche, Referate und Stabsstellen
4) Medizinisch-technische Dienste (z.B. Bereitschaftsdienste, Patientenbegleitdienst, Transportlogistik, IT- und betriebstechnische Dienste)

Beschaffung, Ausgabe, Verwendung und Rücknahme dienstlicher Smartphones

(1) [1]Die Beschaffung von dienstlichen Smartphones oder SIM-Karten geschieht auf Antrag beim Geschäftsbereich Logistik und Zentrale Dienste (G5) mit Genehmigung und Finanzierungszusage durch den Leiter der Struktureinheit. [2]Ausnahmen vom o.g. Personenkreis sind speziell zu begründen und werden durch den Geschäftsbereichsleiter G5 entschieden.

(2) Die Beschaffung dienstlicher Mobilgeräte bzw. SIM-Karten sowie die Verwaltung der zugehörigen Tarifverträge und Rechnungen wird auf der Basis kostenoptimaler Rahmenverträge zentral koordiniert durch die Abteilung Allgemeine Verwaltung (G5.1).

(3) [1]Die Einrichtung und technische Betreuung der dienstlichen Mobilgeräte und ihrer Nutzer erfolgt durch die Abteilung Betriebstechnik (G4.2) in Zusammenarbeit mit dem MRZ. [2]Durch G4.2 erfolgt auch die Einstellung der Telefon-Berechtigungen und Leistungsmerkmale sowie die Durchführung bzw. Organisation von Reparaturen.

(4) [1]Auf Grund finanzieller und technischer Gegebenheiten sowie einer optimalen Service-Organisation wird die Auswahl von Smartphones auf wenige Typen mit einem optimalen Preis-Leistungs-Verhältnis bezüglich Anschaffung und Folgekosten beschränkt. [2]Die diesbezüglichen Hausstandards werden gemeinsam durch G5, G4 und MRZ festgelegt und bei Bedarf aktualisiert.

(5) [1]Die betreffenden Mitarbeiter stellen bei der Abteilung Allgemeine Verwaltung (G5.1) einen schriftlichen Antrag zur Bereitstellung eines Mobiltelefons. [2]Aus einem

bereitgestellten Bestellformular ist das zur Verfügung stehende Gerätespektrum und die anfallenden Kosten ersichtlich. [3]Die Leiter der Struktureinheiten bestätigen den Antrag und übernehmen die Finanzierungszusage der Kosten aus dem eigenen Budget.

(6) G5.1 berät den Antragsteller bei den für den Einsatzfall optimalen Konditionen, aktiviert die SIM-Karten mit den gewünschten Diensten und Funktionen und trifft alle tarifvertraglichen Abreden mit dem Mobilfunk-Anbieter.

(7) [1]Jedes dienstliche Smartphone wird durch das MRZ in das zentrale Mobile-Device-Management-System aufgenommen. [2]Damit werden automatisch allgemein gültige Sicherheitsrichtlinien ausgerollt. [3]Zur Nutzung von Datenservices stellen die Nutzer ggf. einen üblichen Online-Dienstantrag beim MRZ unter:
http://joker/md/nutria/OnlineAntrag => Dienstleistung „Mobile Device Management". [4]Das MRZ beschafft und verwaltet bedarfsgerecht die dazu notwendigen Software-Lizenzen.

(8) [1]Die Nutzer dienstlicher Smartphones sind berechtigt, im UMMD-Campus das interne verschlüsselte WLAN zu nutzen. [2]Die notwendigen WLAN-Profile (Schlüssel) werden automatisch auf die Geräte verteilt.

(9) [1]Die Nutzer verpflichten sich mit ihrem Antrag zur sachgerechten Verwendung des Dienstes und Einhaltung aller datenschutzrechtlichen Bestimmungen. [2]Sie akzeptieren die zentralen Sicherheitseinstellungen, verwenden ausschließlich die zugelassenen Apps. *[3]Das private Telefonieren und die Installation privater Apps und Dienste ist nicht zulässig.*

(10) Eine missbräuchliche Verwendung durch Dritte oder der Verlust eines dienstlichen Smartphones ist unverzüglich folgender Stelle anzuzeigen:

Geschäftsbereich Logistik und Zentrale Dienstleistungen

Abteilung Allgemeine Verwaltung

Tel. 15125

E-Mail: g51@med.ovgu.de

(11) [1]Bei Beendigung des Arbeitsverhältnisses ist im Rahmen der Unterschriftseinholung auf dem Laufzettel personenbezogene Dienst-Telefone in der Abteilung Allgemeine Verwaltung (G5.1) abzugeben. [2]Sonstige nicht personenbezogene Dienstgeräte werden ggf. vom Kostenstellenverantwortlichen des Bereiches eingezogen und verbleiben dort zur Nachnutzung.

Information der Beschäftigten

(1) Jeder Teilnehmer / jede Teilnehmerin erhält bei der Übergabe des Mobilfunktelefons
- eine Beschreibung der Leistungsmerkmale,
- eine Übersicht, welche personenbezogen Daten auf den Servern des Rechenzentrums und im Mobilfunktelefon im Zusammenhang mit der Nutzung des Mobilfunktelefons verarbeitet werden,
- diese Dienstvereinbarung.

(2) Über Neuerungen an Mobilfunktelefonen werden alle Teilnehmer / Teilnehmerinnen unverzüglich über Betriebsmitteilungen durch das Intranet informiert.

(3) Alle Nutzer haben das Recht, vermutete oder tatsächliche Verstöße gegen ihr Recht auf informationelle Selbstbestimmung oder gegen diese Regelung neben der Dienststelle auch dem Datenschutzbeauftragten oder dem Personalrat zu melden.

Schutzvorschriften

(1) [1]Anwesenheits-, Verhaltens- und Leistungskontrollen sowie die Intensivierung der Arbeit von Beschäftigten sind ausdrücklich kein Ziel des Betriebs der Mobilfunktelefone. [2]Soweit dennoch Daten verarbeitet werden, die derartige Kontrollen ermöglichen, vereinbaren Dienststelle und Personalrat ausdrücklich ein Verwertungsverbot.

(2) [1]Die Beschäftigten haben keine Verpflichtung, außerhalb Ihrer Arbeitszeit sowie der dienstplanmäßig für sie persönlich angeordneten Bereitschaftsdienste oder Rufbereitschaften über das Mobiltelefon erreichbar zu sein und auf Anrufe, Mails oder andere Nachrichten zu reagieren. [2]Dienststelle und Personalrat vereinbaren hiermit, dass den Beschäftigten aus der Wahrnehmung dieses Rechtes keine arbeitsvertraglichen Nachteile entstehen und unterbliebene Reaktionen keine arbeitsrechtlichen Sanktionierungen zur Folge haben.

Kontrollrechte des Personalrats

(1) Der Personalrat ist befugt, nach vorhergehender, zumindest aber gleichzeitiger Information der Dienststelle bzw. der betroffenen Abteilung jederzeit die Einhaltung dieser Regelung zu überprüfen.

(2) [1]Der Personalrat hat jederzeit die Möglichkeit, die Räume zu betreten, in denen sich Anlagenteile oder angeschlossene Systeme befinden und dort Kontrollen über die Einhaltung dieser Regelung in Anwesenheit des zuständigen Personals durchzuführen. [2]Dem Personalrat werden auf Anforderung Abfragen des Systemzustandes und der Systemprotokolle ausgedruckt.

(3) [1]Der Personalrat kann verlangen, dass ihm die vollständigen Systemunterlagen der Anlage und der auf diesen durchführbaren Operationen und verwendeten Programme zur Verfügung gestellt werden. [2]Er hat das Recht, alle Dateien der Anlage sowie die von diesen erstellten Ausdrucken einzusehen.

(4) [1]Alle Mitarbeiter und Mitarbeiterinnen der Betriebsführung haben auf die Einhaltung dieser Regelung zu achten. [2]Insofern sind sie gegenüber dem Personalrat im Rahmen der Revisionsprüfung zur Auskunft verpflichtet und berechtigt.

(5) [1]Sofern es zur Wahrnehmung seiner Aufgaben erforderlich ist, kann der Personalrat Sachverständige zu seiner Unterstützung hinzuziehen und/oder entsprechende Schulungen wahrnehmen. [2]Sofern hierfür Kosten entstehen, trägt diese die Dienststelle.

Änderungen

(1) Die Anlagen 1 bis 4 sind Teil dieser Dienstvereinbarung.

(2) [1]Personalvertretungsrechtlich relevante Änderungen der Telekommunikationsanlage gegenüber dem darin beschriebenen Zustand bedürfen der Zustimmung des Personalrats. [2]Dies betrifft insbesondere Schnittstellen und die Leistungsmerkmale der installierten Software.

(3) Bei Änderung der Anlage 3 ergeht eine Information an den Personalrat.

Schlussbestimmungen

1. Salvatorische - Anpassungsklausel

[1]Wird in dieser Dienstvereinbarung auf tarifliche oder außertarifliche Bestimmungen verwiesen, gelten die Bestimmungen in ihrer jeweiligen Fassung. [2]Bei Außerkrafttreten solcher Bestimmungen finden die im Universitätsklinikum Magdeburg A.ö.R. im Übrigen geltenden tarifvertraglichen oder außertarifvertraglichen Regelungen stattdessen Anwendung.

[3]Sollten einzelne Bestimmungen dieser Dienstvereinbarung ganz oder teilweise

unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen oder Teile solcher Bestimmungen unberührt.

2. Inkrafttreten, Wirksamkeit, Kündigung

[1]Die Dienstvereinbarung tritt mit sofortiger Wirkung in Kraft.

[2]Einvernehmlich kann die Dienstvereinbarung jederzeit verändert werden. [3]Jede Vertragspartei hat das Recht, die Dienstvereinbarung mit einer Frist von 3 Monaten zum Quartalsende aufzukündigen. [4]Wird die Dienstvereinbarung von einem Vertragspartner aufgekündigt, bleibt diese bis zum Inkrafttreten einer neuen Vereinbarung wirksam (Nachwirkung).

[5]Alle Änderungen, Ergänzungen sowie die Kündigung dieser Dienstvereinbarung bedürfen der Schriftform. [6]Auch die Abänderung des Schriftformerfordernisses kann nur schriftlich erfolgen.

Magdeburg, den 20.07.2018

Für den Klinikumsvorstand
der Ärztliche Direktor
Dr. med. Jan L. Hülsemann, MBA

Magdeburg, den 18.07.2018

Für den Personalrat
der Vorsitzende
Markus Schulze

Anlagen:

Anlage 1 – Technische Angaben zu den Systemen, Servern, Mobilfunktelefonen, Schnittstellen und der Leistungsmerkmale der installierten Software
Anlage 2 - Ansprechpartner
Anlage 3 - Hausstandards für dienstliche Mobilgeräte
Anlage 4 - Umgang mit privaten Mobilgeräten

Anlage 1 Stand: 12/2017

Technische Angaben zu den Systemen, Servern, Mobilfunktelefonen, Schnittstellen und der Leistungsmerkmale der installierten Software

1) Sicherheitsrisiken ungeschützter mobiler Internet-Zugänge:

Die im privaten Sektor gebräuchlichen mobilen Internetzugänge der Mobilfunk-Provider weisen für den Geschäftssektor keine ausreichenden Sicherheitsmerkmale auf. Die Daten werden in öffentlichen Funknetzen z.T. unverschlüsselt übertragen. Gerätedaten lassen sich zu Cloud-Services der Geräte- und App-Anbieter übertragen. Über mögliche Schadprogramme (Viren, Trojaner) auf den mobilen Endgeräten können Benutzerdaten ausgespäht und ggf. auch im Firmen-Intranet missbraucht werden. Viele der verwendeten Apps besitzen gefährliche Sicherheitslücken, die von App-Anbietern und Hackern zum Abgreifen von Daten ausgenutzt werden können. Auch bei Verlust eines ungesicherten Mobilgerätes besteht die Gefahr, dass die lokal gespeicherten Daten in unbefugte Hände gelangen.

Nur wenn interne Daten sicher übertragen und gespeichert und Zugangsberechtigungen mit den unternehmenseigenen Rollen synchronisiert werden, kann ein wirksamer Schutz von Unternehmensdaten gewährleistet werden.

Die mobile Datenkommunikation an der UMMD ist hochgradig schutzbedürftig (s. IT-Sicherheitsgesetz, KRITIS-Verordnung) und bedarf eines verantwortungsvollen Umgangs durch IT-Dienstanbieter und Nutzer. Eine ungeschützte mobile Datenkommunikation scheidet deshalb für betrieblichen Geschäftsverkehr im Klinikums-Umfeld aus.

Ein umfassendes Risiko-Management, das mit den flexiblen Ansprüchen der Benutzer und den begründeten Sicherheitsbedürfnissen der Unternehmens-IT verträglich ist, kann nur durch ein zentrales Mobilgeräte-Management-System erreicht werden, das von vornherein auf Sicherheit ausgerichtet ist.

2) Realisierungsstand an der UMMD / Blackberry-Universal-Endpoint-Management:

Mit dem Start der Verwendung sicherer dienstlicher BlackBerry-Smartphones ab 2010 wurde an der UMMD der lokale Blackberry-Enterprise-Service in den Versionsschritten BES3, BES4, BES5, BES10 und BES12 etabliert und inzwischen zum Blackberry-Universal-Endpoint-Mangement (BUEM12) ausgebaut. Diese Software bestimmt von Beginn an den Standard für eine sichere Mobilkommunikation für Regierungen, Behörden, Kliniken und sicherheitsrelevante Unternehmen. Die verwendeten VPN-Technologien, die abgesicherte weltweite Netzinfrastruktur geben auch heute noch das technisch und wirtschaftlich machbare Maß vor.

Blackberry-Infrastruktur und -Software-Lösungen besitzen weltweit Sicherheitszertifikate offizieller, für den Datenschutz zuständiger Stellen. Aktuelle Marktanalysen bescheinigen Blackberry bis heute die Marktführerschaft bei Leistungsparametern, Sicherheit und Wirtschaftlichkeit.

Auf die sich rasant entwickelnde Smartphone-Landschaft reagiert der Software-Hersteller durch Ausweitung der Mobilgeräte-Basis und stetige Weiterentwicklung der Server-Software. Der Enterprise-Server, heute in der Version BUEM12, hat sich als universelle zentrale Managementplattform für alle mobilen Endgeräte mit gängigen Betriebssystemen (Android, iOS, BB-OS10 u.a.) konsolidiert, mit einem inzwischen auch für Android und iOS gleichwertigen Sicherheitsniveau.

Mit erfolgten Akquise von MDM- und Security-Anbietern und der Integration ihrer Dienste in die BUEM12-Plattform wird aktuell das Portfolio abgesicherter mobiler Anwendungen signifikant erweitert. Damit werden an der UMMD folgende Grundfunktionalitäten abgedeckt:

- Mobile-Device-Management (MDM):
  Verwaltung von Geräte-Grundfunktionen, Sicherheitsrichtlinien und Berechtigungen, automatische Geräteaktivierungen, Fernlöschung bei Geräteverlust u.a.
- Mobile Security Management (MSM):
  Ende-zu-Ende-Sicherheit durch Verschlüsselung der Kommunikation und Datenspeicherung, Passwort- und Zertifikatsverwaltung.
  Sichere Trennung von persönlichen und dienstlichen Apps und Daten durch Container-Lösungen.
- Universal-Device-Management (UDM):
  Einheitliche Bereitstellung der Sicherheitsfunktionen und -Apps für Endgeräte mit unterschiedlichen Betriebssystemen.
- Mobile Application Management (MAM):
  Automatische Verteilung von unternehmensspezifischen Apps und deren automatisierte Installation und Konfiguration.
- Mobile-Content-Management (MCM):
  Sichere Bereitstellung von Dateidiensten und Umsetzung von Sicherheitsrichtlinien zum Umgang mit diesen Daten.
- Mobile User Management (MUM):
  Integration der Nutzerverwaltung in Unternehmens-Verzeichnisdienste.
  Automatische Synchronisation von Rollen und Berechtigungen.
  Automatisierung von Verwaltungsaufgaben für Endbenutzer und IT-Administratoren.

Zu den o.g. Grundfunktionen kommen sichere Anwendungen und Schnittstellen hinzu: z. B. BB-Work-Apps, Google-Android-for-Work, Samsung-KNOX, Apple-DEP und Business-Apps für File-Sharing, Messaging, Kollaboration, Alarmierung und Katastrophenschutz. Dies ermöglicht auch zukünftig bedarfsgerechte Funktionserweiterungen.

Der klinikinterne Blackberry-Server der UMMD besitzt eine Schnittstelle zu den Active-Directory- und Exchange-Servern, wodurch die mit Office-PCs bearbeiteten Daten und Anwendungen (z.B. Emails, Kalender, Kontakte) mit den mobilen Endgeräten der Nutzer automatisch synchronisiert werden können. Die Sicherheits-Richtlinien von Intranet und dienstlichem Endgeräte-Bereich werden hierbei durchgängig von der IT-Administration nach Unternehmensrichtlinien eingestellt.

Durch die Infrastruktur können für alle mobilen Anwendungen durchgängig sichere Kommunikations-Kanäle mit einer Ende-zu-Ende-Verschlüsselung vom mobilen Endgerät bis zum Zugangsserver im Klinikums-Intranet bereitgestellt werden.

Der Blackberry-UEM-Service ist auf den Servern BES1, GEMSCO, GEMSDB installiert. Alle Serverkomponenten laufen als virtuelle Maschinen in der zentralen VMWARE-Infrastruktur des MRZ.

Für alle Nutzungsszenarien in der UMMD sind die Anforderungen an den Datenschutz und die Datensicherheit für mobile Geräte und Anwendungen durchsetzbar. Durch den skalierbaren Leistungs- und Funktionsumfang und moderne mobile Kommunikations-Anwendungen ist die Infrastruktur zukunftsfähig, langfristig wirtschaftlich und kann auf die wachsenden Anforderungen aus Klinikum und Fakultät weiterhin adäquat und flexibel reagieren.

Weiterführende Informationen zum Dienst „Mobile Device Management / BUEM": http://www.mrz.ovgu.de/mdm.html

3) Sicherheit dienstlicher Mobilgeräte an der UMMD

In der UMMD wurden dienstliche Mobilgeräte bis 2016 nur in eingeschränktem Umfang verwendet, z.B. für medizinische und technische Bereitschaftsdienste, den Patientenbegleitdienst, den externen Krankentransportdienst, die Transportlogistik, die Essenbestellung (MUKS) für Patienten. Außerdem existieren einige Notfall-Handys mit reiner Telefonfunktion.

Der Klinikumsvorstand beabsichtigt die bedarfsgerechte Ausweitung von dienstlichen Mobilgeräten für alle Dienstgruppen. Dabei ist zu berücksichtigen, dass die alten analogen PSA-Pager mittelfristig durch moderne Multifunktions-Geräte ersetzt werden, die ebenfalls bidirektionale Sprach- und Datendienste im WLAN und Mobilfunknetz erlauben.

Mit der im Einsatz befindlichen Container-Lösung zur sauberen Trennung zwischen persönlichen und dienstlichen Daten und Apps lassen sich alle Datenschutz-Anforderungen aus Nutzer- und Betreibersicht erfüllen, d.h. der Firmen-Administrator erhält Administrations-Hoheit auf den dienstlichen Teil des Mobilgerätes, ohne auf persönliche Daten zugreifen zu können, und die dienstlichen Daten auf dem Gerät sind jederzeit passwortgeschützt und verschlüsselt und damit gegen Zugriff Dritter gesichert.

Der Lebenszyklus von Standard-Mobilgeräten beträgt derzeit 2-3 Jahre. Danach ist oft durch technischen und moralischen Verschleiß ein Austausch nötig. Aus Sicht der TK- und IT-Administration und Absicherung der Service-Qualität und Folgekosten ist für dienstliche Mobilgeräte die Einschränkung auf wenige leistungsfähige Hersteller notwendig. Das ist darin begründet, dass es insbesondere für Android-Geräte eine unüberschaubare Anzahl von Herstellern und Betriebssystem-Varianten gibt, wobei jeder Hardware-Hersteller um den Betriebssystem-Kern herum eigene Oberflächen und Systemfunktionen baut. Die sicherheitsrelevanten Betriebssystem-Updates und Security-Patches werden von den meisten Herstellern nicht zeitnah und nur für einen begrenzten Zeitraum (ca. 1 Jahr) zur Verfügung gestellt. Ein Gerät ohne System- und Sicherheits-Update ist ein unsicheres Gerät.

Aus den genannten Gründen sind konkrete Herstellervorgaben im Hausstandard notwendig (s. Anlage 3).

Anlage 2

Allgemeine Ansprechpartner:

- Geräte-Beschaffung und Tarife:
  Geschäftsbereich Logistik und Zentrale Dienstleistungen
  Abteilung Allgemeine Verwaltung
  Tel. 15125
  E-Mail: g51@med.ovgu.de

- Geräte-Ersteinrichtung und -Reparatur:
  Geschäftsbereich Technik und Bau
  Abteilung Betriebstechnik
  SG Telekommunikation und Leittechnik
  Tel. 15154
  E-Mail: fernmelde@med.ovgu.de

- Mobile Datendienste:
  Medizinisches Rechenzentrum
  Abteilung Kommunikation & Netze
  Tel. 15720
  E-Mail: netmaster@med.ovgu.de

Anlage 3

Hausstandards für dienstliche Mobilgeräte (Stand 01/2018)

Wegen der Sicherheitsvorgaben und einem langfristig zuverlässigen und kostenoptimalen Betrieb dienstlicher Mobilgeräte sind Hausstandards notwendig. Diese werden nach umfangreichen Tests und Wirtschaftlichkeitsbetrachtungen permanent überprüft und ggf. angepasst. Dabei sind der Stand der Technik und weitere Kriterien wie Gerätesicherheit, Wirtschaftlichkeit, Nachhaltigkeit sowie eine optimale Service-Organisation zu berücksichtigen.

Eine Beschränkung auf einige Geräte-Hersteller und -Typen ist deshalb notwendig, begrenzt auf Marktführer mit einem möglichst breiten Geräte-Portfolio, einer zuverlässigen Sicherheits-Strategie und langfristiger Hardware-Perspektive.

Die Hausstandards werden durch ein internes Betreiber-Gremium (Abteilung Allgemeine Verwaltung, Abteilung Betriebstechnik, Medizinisches Rechenzentrum) auf Grund technischer und wirtschaftlicher Rahmenbedingungen und Betriebserfahrungen festgelegt und bei Bedarf aktualisiert.

Allgemeine Geräte-Merkmale und Mindestkriterien:

- Touchscreen, LED- oder AMOLED-Display mit HD-Auflösung (Kategorie A und B)
- Betriebssystem Android 6.0 oder höher
- Schnittstellen: LTE/UMTS/GSM, WLAN 2,4 und 5GHz, Bluetooth, USB
- Speicher: >16 GB, erweiterbar bis 256 GByte
- 2 Kameras
- Leichtes, schlankes, aber robustes Design
- Stromsparender Betrieb und optimale Akku-Laufzeiten
- Wasser- und Staubschutz, (IP-Zertifizierung) Desinfizierbarkeit
- Abgesichertes Service-Konzept mit Dienstanbieter, einheitlicher Ansprechpartner für Geräte und Tarifverträge
- Geräte-Fabrikat und Typ wird auch nach wirtschaftlichen Gesichtspunkten, wie Preis/Leistungs-Verhältnis, Nachhaltigkeit und Folgekosten gewählt
- Möglichst kostengünstige Tarife und Tarifoptionen lt. Rahmenverträgen mit Mobilfunk-Anbietern.

Leistungsklassen je nach Anwendung:

- Kategorie A: Obere Mittelklasse, Display >5,2"
- Kategorie B: Untere Mittelklasse, Display < 5"
- Kategorie C: Kompaktes und robustes Einsteigergerät, Display < 5"

Mobilfunk-Tarife:

Die Wirtschaftlichkeit des Betriebes wird über kostenoptimale Tarif-Rahmenverträge gewährleistet. Bei Neubeschaffungen von Endgeräten werden mögliche Synergie-Effekte von Hardware- und Tarif-Kombinationen berücksichtigt.

Kostenstellenverantwortung (laufende Telekommunikationskosten): G5.1

Aktuell: Telekom/DFN-Rahmenvertrag RV37359
Europaweite Ausschreibung des DFN, gültig ab 01/2017

Anlage 4

Umgang mit privaten Mobilgeräten:

Die Nutzung privater Smartphones für dienstliche Belange wird wie folgt geregelt:

1) Die Nutzung privater Smartphones oder Tablet-Computer für dienstliche Datendienste ist in eingeschränktem Umfang möglich. Das betrifft die grundlegenden Exchange-Dienste wie E-Mail, Kontakte und Kalender und einen abgesicherten Internet-Zugang. Die Nutzung anderer Dienste und der Zugriff auf sonstige interne Daten sind nicht zulässig.
2) Durch das zentrale Mobile-Device-Management und die darüber bereit gestellten dienstlichen Container-Apps wird eine datenschutzkonforme sichere Trennung von dienstlichen und persönlichen Daten gewährleistet. Das schließt ein, dass die Dienststelle keine privaten Daten auf dem Endgerät einsehen kann.
3) Die Nutzung geschieht ausschließlich auf eigenen Wunsch der Mitarbeiter. Eine Pflicht zur Dienstnutzung besteht nicht. Der Nutzer ist demnach nicht verpflichtet, über sein privates Mobilgerät erreichbar zu sein.
4) Der Nutzer kann den Empfang von E-Mails auf dem Gerät jederzeit durch Beenden der dienstlichen Apps unterbrechen. Darüber hinaus kann der Nutzer den Dienst und die Geräteverwaltung dauerhaft beenden, durch selbständiges Deaktivieren seines Gerätes und Löschen der geschäftlichen Apps. Nach Ausscheiden eines Mitarbeiters aus dem Arbeitsverhältnis erlischt die Nutzungserlaubnis für den Service automatisch, und der Zugriff auf dienstliche Daten ist nicht mehr möglich.
5) Zur Nutzung der dienstlichen Datenservices auf einem privaten Endgerät stellen die Mitarbeiter einen personenbezogenen Online-Dienstantrag mit Genehmigung des Leiters der Struktureinheit.
   http://joker/md/nutria/OnlineAntrag -> Mobile-Device-Management.
6) Die Nutzer verpflichten sich mit ihrem Antrag per Unterschrift zur sachgerechten Verwendung des Dienstes und Einhaltung aller datenschutzrechtlichen Bestimmungen. Sie akzeptieren die zentralen Sicherheitseinstellungen.
7) Nach erfolgter Genehmigung des Antrages durch den MRZ-Leiter können die berechtigten Mitarbeiter auf Basis eines privaten Mobilfunk-Vertrages ein dafür geeignetes Mobiltelefon gemäß 1) nutzen.
8) Das MRZ übernimmt die Unterstützung der Nutzer bei der Geräteaktivierung und ist im Zusammenhang mit dem Mobile-Device-Management den Nutzern gegenüber weisungsberechtigt. Bei unsachgemäßer Benutzung und Verstößen gegen die Unternehmensrichtlinien kann der Zugang zum Dienst gesperrt und die dienstlichen Daten gelöscht werden. Die persönlichen Daten und sonstigen Telefonfunktionen werden davon nicht tangiert.
9) Die Mitarbeiter tragen die aus dem Mobilfunk-Vertrag anfallenden Kosten selbst. Die Kosten für die Mobile-Device-Management-Lizenzen übernimmt die Dienststelle.
10) Die Dienststelle übernimmt keine Haftung für Verpflichtungen, Risiken oder Schäden aus dem privaten Mobilfunkvertrag und ist nicht zuständig für Fehlfunktionen und Störungen an privaten Mobilgeräten, soweit diese nicht in Zusammenhang mit dem Mobile-Device-Management stehen. Außerdem übernimmt sie keine Garantie für die Gerätefunktion, haftet nicht für Geräteschäden bzw. Verlust von Gerätedaten. Für deren Schutz und Datensicherung sind die Nutzer selbst zuständig.