DATENSCHUTZANFORDERUNGEN UND LÖSUNGSANSÄTZE BEIM EINSATZ MOBILER GERÄTE IM GESUNDHEITSWESEN - ORGANISATORISCHE ANFORDERUNGEN

Dr. Dipl. Inform. Bernd Schütze, M.D., LL.B.

Workshop der GMDS-AG „Datenschutz in Gesundheitsinformationssystemen“ am 2014-09-09, 59. GMDS-Jahrestagung

HEALTHCARE SOLUTIONS

DATENSCHUTZ IM MOBILEN: DIE SICHT DES INFORMATIKERS

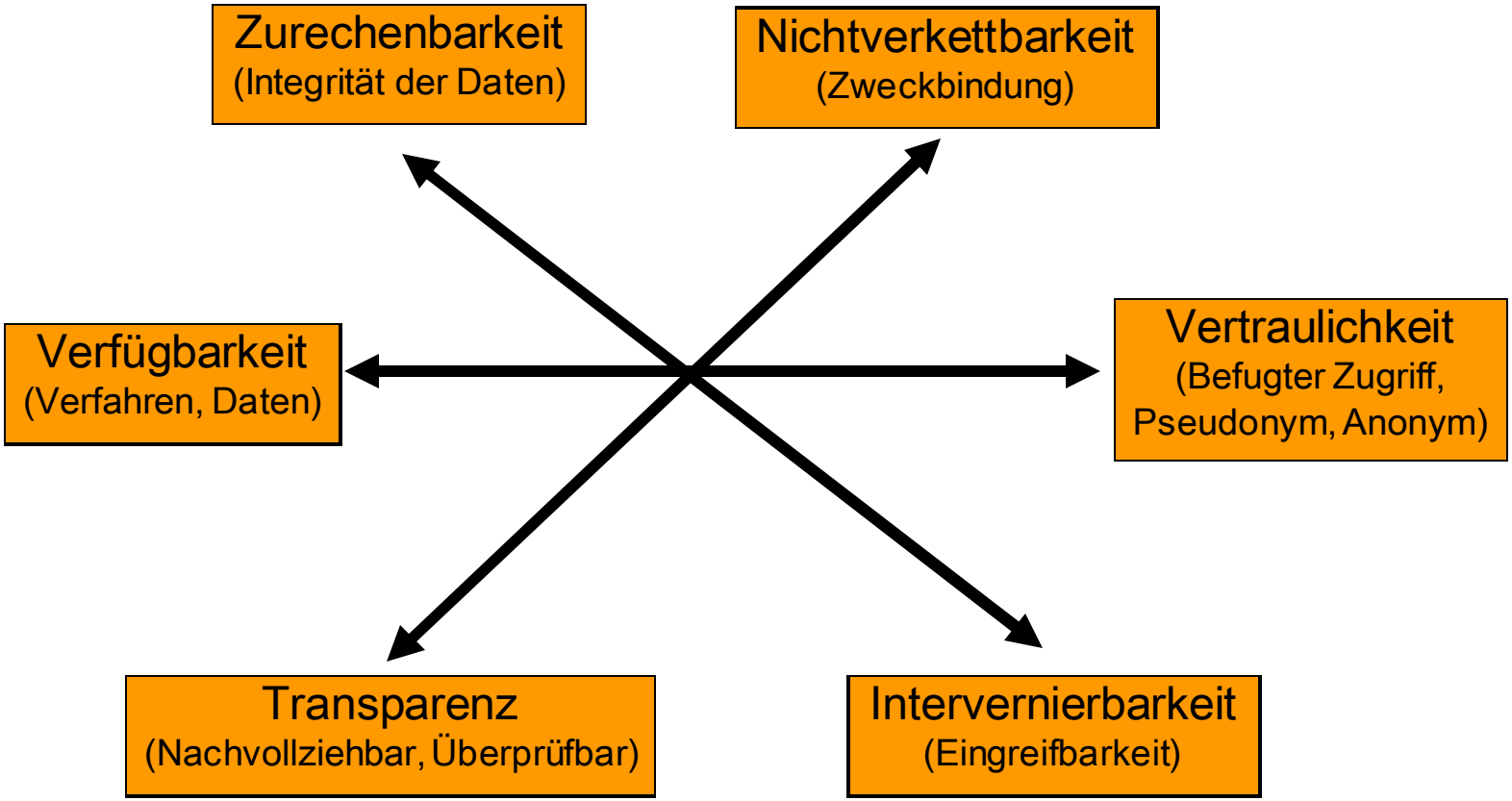
OSI-Modell		Anzuwendende Gesetze
7	Anwendung	(Gesundheits)- Datenschutzgesetze (Bundesrecht / Landesrecht / Kirchenrecht)
6	Darstellung	Telemediengesetz
5	Sitzung	
4	Transport	Telekommunikationsgesetz
3	Vermittlung	
2	Sicherung	
1	Bitübertragung	

SCHICHT 7:
DIE DATENSCHUTZGESETZE

- **EU**
  - Europäische Grundrechte-Charta
  - Datenschutz-Richtlinie
    Wirkung über Umsetzung in deutsche Gesetze
  - Datenschutz-Verordnung
    (derzeit im Entwurf, sie würde unmittelbar gelten und deutsches Recht ersetzen)
- **Bundesdatenschutzgesetz (BDSG)**
  - Privatpersonen
  - Privatwirtschaft
  - Bundesbehörden
- **Kirchliche Datenschutzgesetze**
  - Einrichtungen der evang. und kath. Kirche
- **Landesdatenschutzgesetze**
  - öffentliche Verwaltung in Land und Kommunen
- **Spezialgesetze (Vorrang vor allg. Gesetzen)**
  - TeleMedienGesetz
  - TeleKommunikationsGesetz
  - Landeskrankenhausgesetze
  - Gesundheitsdatenschutz
  - Hochschulgesetz
  - SGB, AO, Polizeigesetz, Passgesetz, Personalausweisgesetz, Aufenthaltsgesetz, LandesMeldeGesetz, Landesverwaltungsgsetz, ..

- **Rechtmäßigkeit der Datenverarbeitung**
  - Gesetzliche Grundlagen
  - Einwilligung
- **Grundsatz der Zweckbindung**
- **Grundsatz der Erforderlichkeit**
- **Grundsatz der Datenvermeidung und Datensparsamkeit**
- **Grundsatz der Transparenz**
- **Grundsatz der klaren Verantwortlichkeiten**
- **Grundsatz der Kontrolle**
- **Grundsatz der Gewährleistung der Betroffenenrechte**
  - Verbot der Profilbildung
  - Verbot der Datensammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- **Nutzung pseudonymisierter oder anonymisierter Daten**
- **Verpflichtung zum Schutz der Daten**

ZIELE DES DATENSCHUTZES – ANTAGONISTEN ZUEINANDER?



ANFORDERUNGEN

1. **Gesundheitsdaten, die einer Person zugeordnet werden können, sind**
   - Sicher aufzubewahren (Verschlüsselte Dateiablage)
   - Getrennt von anderen Daten aufzubewahren
   - Sicher zu übertragen (Verschlüsselten Übertragungsweg beachten)
   - Ggfs. Verfügbarkeit zu gewährleisten
     (Cave: Gesundheitsschaden bei Nicht-Verfügbarkeit?)
   - Nachweispflichtig
     - ✓ Bzgl. Zugriff auf die Daten (Logdatei)
     - ✓ Änderung der Daten (Versionskontrolle)
2. **Bedenken: Eine Produkt kann ein Medizinprodukt werden (In-House-Verfahren), woraus weitere Anforderungen resultieren**

RICHTLINIE MOBILE GERÄTE: ARBEITSZEIT

gmds
Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

An Regelung der Arbeitszeit denken
(Urteil Arbeitsgericht Berlin vom 22. März 2012 AZ 54 BV 7072/11)

- Der Arbeitgeber hat die Arbeitszeit seiner Beschäftigten zu kontrollieren.
- Der Arbeitgeber darf außerhalb der Arbeitszeit geleistete Arbeit der Beschäftigten nicht entgegennehmen, nicht einmal dulden.
- Schon das Lesen dienstlicher E-Mails kann Arbeitsleistung sein.
- Erlangt der Arbeitgeber Kenntnis von Freizeitarbeit seiner Beschäftigten muss er sie unterbinden.
- Duldet der Arbeitgeber Freizeitarbeit seiner Beschäftigten - z.B. mit mobilen Geräten - muss er den Betriebsrat beteiligen.
- Duldet der Arbeitgeber Freizeitarbeit ohne den Betriebsrat zu beteiligen, kann dieser Unterlassung verlangen. Der BR kann sich auf seine Mitbestimmungsrechte aus § 87 Abs.1 Nr.1 und Nr.3 BetrVG berufen

Merke: Der Arbeitgeber genügt seiner Durchführungsverpflichtung mithin nicht, wenn er Arbeitnehmern die Entscheidung überlässt, ob sie außerhalb der Arbeitszeit E-Mails bearbeiten.

RICHTLINIE MOBILE GERÄTE: ARBEITSZEIT, BEISPIEL

1. Wahrend des Urlaubs soll auf dienstliche Telefonate, sowie Lesen und Bearbeiten von beruflichen E-Mails verzichtet werden.
2. Der Arbeitgeber hegt bei freiwilliger Nutzung in der Freizeit und am Wochenende keine Erwartung für die umgehende Beantwortung und Bearbeitung von E-Mails.
3. Der Arbeitgeber fordert seine Beschäftigten auf, sich selbst klare E-Mail-Zeiten zur Bearbeitung zu setzen.
4. Jeder Anwender sollte sich bewusst fragen, ob ein E-Mail-Versand in der Freizeit notwendig ist.
5. Ausnahmen bilden Krisensituationen und Situationen, in denen ein unmittelbares Handeln erforderlich ist. Hier ist die direkte Kommunikation per Anruf zu bevorzugen.
6. Der Arbeitnehmer achtet darauf, dass in der Freizeit geleistete Arbeit in der Arbeitszeiterfassung erfasst wird, so dass ein Ausgleich der geleisteten Arbeitszeit durch den Arbeitgeber ermöglicht wird..

RICHTLINIE MOBILE GERÄTE: UMGANG BEI MEETINGS

- Bleiben Geräte angeschaltet?
- Werden Anrufe angenommen?
- Werden E-Mails beantwortet?

RICHTLINIE MOBILE GERÄTE: UMGANG BEI MEETINGS, BEISPIEL

1. Zu Beginn des Meetings soll das gemeinsame Vorgehen bzgl. des Umgangs mit mobilen Arbeitsmitteln abgestimmt und ggfs. begründete Ausnahmen definiert werden.
2. Das Ausschalten der mobilen Arbeitsmittel in Sitzungen und Teammeetings ist eine Frage des Respekts Anderen gegenüber sowie eine Frage des Anspruchs, der Effektivität und der Leistungsorientierung eines Meetings.

RICHTLINIE MOBILE GERÄTE: TECHNISCHE ANFORDERUNGEN

- Betriebssystem
- Benutzerkennwörter
- Welche Geräte dürfen ins Netz

RICHTLINIE MOBILE GERÄTE: TECHNISCHE ANFORDERUNGEN, BEISPIEL

1. Die Geräte müssen unter folgenden Betriebssystemen laufen: Android 2.3 oder höher, IOS 4.x oder höher.
2. Benutzerkennwörter zu den Geräten dürfen nur in verschlüsselten Kennwortspeichern aufbewahrt werden.
3. Die Anwender müssen ein sicheres Kennwort für die Geräte konfigurieren, das den Anforderungen der Kennwortrichtlinie von <Unternehmen X> genügt. Das Kennwort darf nicht für andere Anwendungen im Unternehmen verwendet werden.
4. Nur Geräte, die von der IT-Abteilung verwaltet werden, dürfen direkt mit dem Unternehmensnetzwerk verbunden werden.

RICHTLINIE MOBILE GERÄTE: PFLICHTEN

- Zugriff auf Daten durch Anwender
- Meldepflicht bei Geräteverlust
- Unbefugter Zugriff auf Daten
- Umgang mit Jailbreak & Co
- Softwareinstallation (ins. Raubkopien)
- Welche Geräte dürfen an welchen Computer angeschlossen werden?
- Vermischung provate/dienstliche Nutzung?

RICHTLINIE MOBILE GERÄTE: PFLICHTEN, BEISPIEL

1. User dürfen nur unternehmensrelevante Daten auf die Mobilgeräte laden.
2. Abhanden gekommene oder gestohlene Geräte müssen der IT-Abteilung von <Unternehmen X> umgehend gemeldet werden.
3. Vermutet ein User, dass ein unbefugter Zugriff über Mobilgeräte auf Unternehmensdaten erfolgt ist, muss er dies der IT-Abteilung in Einklang mit Melderichtlinien in <Unternehmen X> mitteilen.
4. Der Einsatz von Geräten mit Jailbreak oder Software/Firmware zum Zugriff auf eigentlich nicht für den User vorgesehene Funktionen ist nicht gestattet.
5. User dürfen keine Raubkopien oder illegalen Inhalte auf die Geräte laden.

RICHTLINIE MOBILE GERÄTE: PFLICHTEN, BEISPIEL

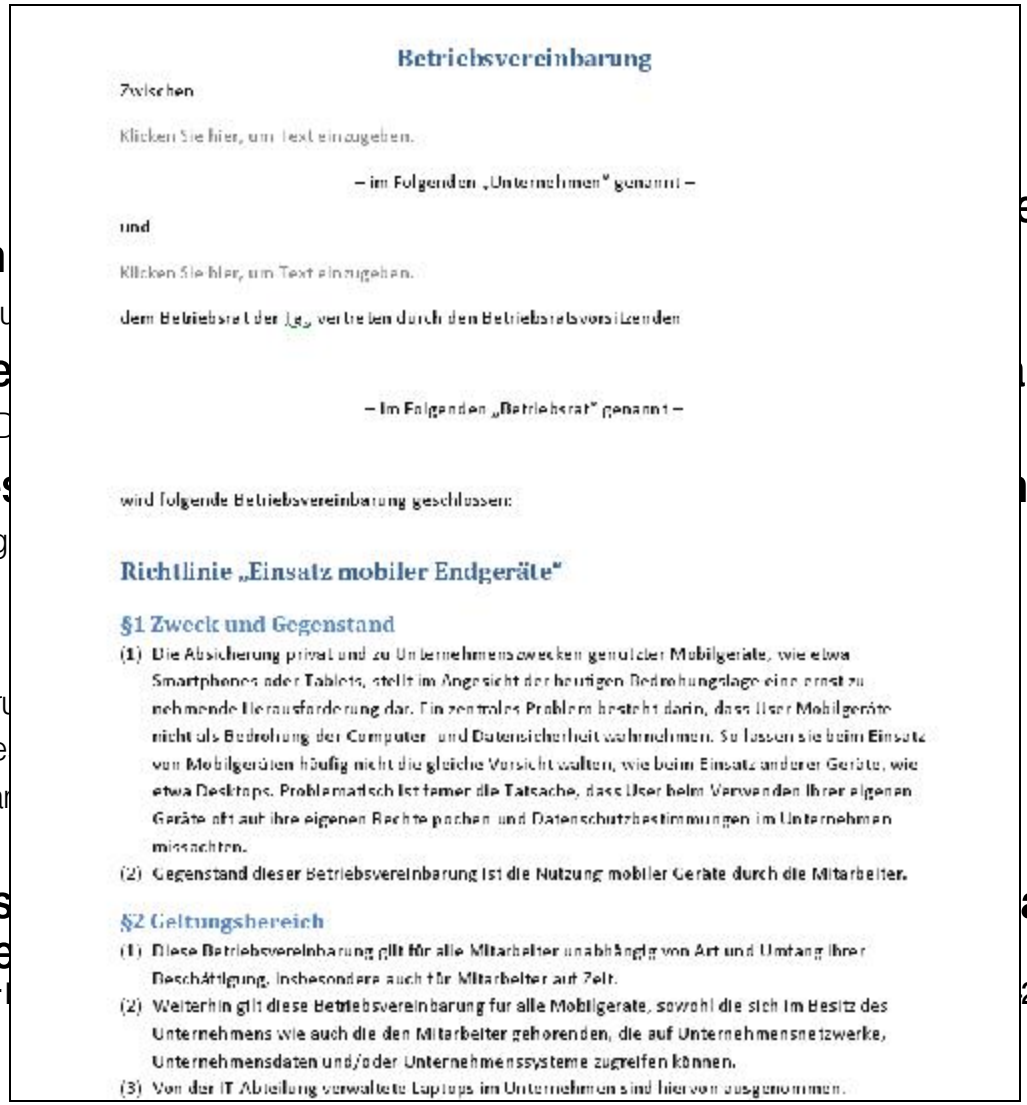
6. Sämtliche installierten Anwendungen müssen offiziellen, vom Entwickler des jeweiligen Betriebssystems autorisierten Quellen entstammen. Es darf kein Code von fragwürdigen Quellen installiert werden. Die IT-Abteilung von <Unternehmen X> kann Ihnen im Zweifel mitteilen, ob eine Anwendung vertrauenswürdig ist.
7. Die Geräte sind mit den aktuellen Patches des Herstellers oder Netzwerks auszustatten. Sie sollten mindestens einmal pro Woche überprüfen, ob neue Patches vorhanden sind, und mindestens einmal im Monat Patches installieren.
8. Die Geräte dürfen nicht an Computer angeschlossen werden, die nicht über aktuellen, aktivierten Malwareschutz verfügen und gegen Unternehmensrichtlinien verstoßen.

RICHTLINIE MOBILE GERÄTE: PFLICHTEN, BEISPIEL

9. Geräte müssen in Einklang mit den Compliance-Standards von <Unternehmen X> verschlüsselt werden.
10. Bei der Verknüpfung von privaten und professionellen E-Mail-Konten ist stets Vorsicht geboten. Unternehmensdaten dürfen nur über die Unternehmens-E-Mail-Adresse versendet werden. Hegt ein User den Verdacht, dass Unternehmensdaten über ein persönliches E-Mail-Konto (im E-Mail-Text oder als Attachment) verschickt wurden, so muss er die IT-Abteilung von <Unternehmen X> umgehend darüber in Kenntnis setzen.
11. User dürfen keine Geräteinhalte (wie etwa Mediendateien) auf Unternehmenscomputern sichern oder synchronisieren, sofern dies nicht zu Unternehmenszwecken erfolgt.

BETRIEBSVEREINBARUNG

- **Wenn Einsatz … eibung enthalten, liegt i.d.R. ein …**
  - Personalvertretu…
- **Individualvere… r**
  - Cave: Bei BYOD…
- **Je nach einges… ungsmöglichkeit**
  - → Zustimmung…
- **Inhalt**
  - Welche Apps?
  - Diebstahlsicheru…
  - Was darf wo ge…
  - Antivirenprogra…
  - …
- **Cave: Vorauss… atenschutzrechtlich als vorrangige…**
  (Hinweise hierzu unter… 2009.pdf)



Betriebsvereinbarung

Zwischen

Klicken Sie hier, um Text einzugeben.

– im Folgenden „Unternehmen" genannt –

und

Klicken Sie hier, um Text einzugeben.

dem Betriebsrat (der i.g., vertreten durch den Betriebsratsvorsitzenden

– im Folgenden „Betriebsrat" genannt –

wird folgende Betriebsvereinbarung geschlossen:

Richtlinie „Einsatz mobiler Endgeräte"

§1 Zweck und Gegenstand

(1) Die Absicherung privat und zu Unternehmenszwecken genutzter Mobilgeräte, wie etwa Smartphones oder Tablets, stellt im Angesicht der heutigen Bedrohungslage eine ernst zu nehmende Herausforderung dar. Ein zentrales Problem besteht darin, dass User Mobilgeräte nicht als Bedrohung der Computer- und Datensicherheit wahrnehmen. So lassen sie beim Einsatz von Mobilgeräten häufig nicht die gleiche Vorsicht walten, wie beim Einsatz anderer Geräte, wie etwa Desktops. Problematisch ist ferner die Tatsache, dass User beim Verwenden Ihrer eigenen Geräte oft auf ihre eigenen Rechte pochen und Datenschutzbestimmungen im Unternehmen missachten.

(2) Gegenstand dieser Betriebsvereinbarung ist die Nutzung mobiler Geräte durch die Mitarbeiter.

§2 Geltungsbereich

(1) Diese Betriebsvereinbarung gilt für alle Mitarbeiter unabhängig von Art und Umfang ihrer Beschäftigung, insbesondere auch für Mitarbeiter auf Zeit.

(2) Weiterhin gilt diese Betriebsvereinbarung für alle Mobilgeräte, sowohl die sich im Besitz des Unternehmens wie auch die den Mitarbeiter gehörenden, die auf Unternehmensnetzwerke, Unternehmensdaten und/oder Unternehmenssysteme zugreifen können.

(3) Von der IT Abteilung verwaltete Laptops im Unternehmen sind hiervon ausgenommen.

BETRIEBSVEREINBARUNG

- Technische Anforderungen analog Richtlinie
- Pflichten der Anwender analog Richtlinie
- Regelungen analog zur „normalen“ PC-Arbeit
  - Regelung bzgl. Auswertung Protokollauswertung
  - Zugriff auf Daten (insbesondere, wenn private Nutzung nicht verboten ist)
  - Ggfs. Regelungen zu Lokalisationsmöglichkeiten (Stichwort: verlorenes Gerät)
- Mißbrauchskontrolle
- Inkrafttreten & Co.

BETRIEBSVEREINBARUNG MIßBRAUCHSKONTROLLE, BEISPIEL

1. Alle Mitarbeiter haben das Recht, den vermuteten oder tatsächlichen Missbrauch und Missbrauchsversuche beim Einsatz der mobilen Geräte durch Mitarbeiter dem Unternehmen mitzuteilen.

SONDERFALL BYOD

- **Krankenhaus wird einerseits Mitarbeitern die Nutzung privater Geräte langfristig nicht verweigern können**
- **Aber: Auf dem Mitarbeiter gehörende Geräte hat der Arbeitgeber keine Weisungsbefugnis**
  - Auf diesen Geräten gespeicherte Patientendaten befinden sich daher prinzipiell nicht in der Einrichtung
  - Die Patientendaten werden ggfs. übermittelt
  - ➔ Übermittlung = Einwilligung des Patienten nötig!
  - ➔ Daher Patientendaten nur dort speichern, wo der Arbeitgeber völlige Verfügungsgewalt über die Daten behält
- **Regelungen ähnlich „Telearbeitsplatz“ erforderlich**
- **Erster Anhalt, wie das Unternehmen bzgl. BYOD-Einführung dasteht, durch IBM BYOD Check: http://www.challenge-check.ch/byod/**

REGELUNGSBEDARF BYOD

- **Regelung zur Datenverarbeitung**
  - Verarbeitung personenbezogener Daten ausschließlich an orten, an denen der Schutz der Daten gewährleistet ist
  - Beispiel: Diktate von Patientenbehandlungen möglichst nicht in der Wartehalle des Flughafens ;-)
  - Backup der Unternehmensdaten: ist gewährleistet, dass keine privaten Daten im Backup enthalten sind?
- **Zustimmung bzgl. Zugriff auf privates mobiles Endgerät erforderlich ↔ Kontrollmöglichkeit des Arbeitgebers bei privater Hardware entfällt („Computer-Grundrecht“, BVerfG 27.02.2008)**
  - Installation der unternehmensinternen MDM-Lösung
  - Installation Virenscanner & Co.
  - Datenlöschung bei Verlust
  - Auswertung von Protokolldateien

REGELUNGSBEDARF BYOD

- **Regelungen bzgl. Lizenzrecht**
  - Installation von Software des Unternehmens auf privater Hardware vs. Urheberrecht (Evtl. Hinweis des Herstellers „Nutzung nur auf Rechnern, die im Eigentum des Lizenznehmers stehen“?)
  - Nutzung der privat gekauften Lizenzen für dienstliche Zwecke?
- **Installation eigener Software**
  - Darf Besitzer beliebige Software auf sein Gerät aufspielen?
  - Mit welcher installierten Software darf er noch ins Unternehmensnetz?
- **Regelung bzgl. Nutzung des mobilen Endgerätes durch Dritte, z.B.**
  - durch Familienangehörige: Kind spielt mit iPad, ...
- **Haftungsrecht**
  - Verlust/Beschädigung Smartphone während Arbeit
  - Datenveränderung (§303a StGB), z.B. private Daten und Virenschutz des Unternehmens
  - ...

REGELUNGSBEDARF BYOD

- **Steuerrechtliche Fragen**
  - Vergütungsanspruch des Mitarbeiters für die betriebliche Nutzung?
  - Geldwerter Vorteil
  - ...
- **Reparatur des Gerätes**
  - Einschicken durch Besitzer?
  - Alternativ: Ersatz durch Arbeitgeber?
- **Entsorgung des Gerätes**
  - Entsorgung durch Unternehmen?
  - Kauf des mobilen Endgerätes durch Unternehmen?
  - Verkauf durch Eigentümer an Dritte möglich? (Z.B. eBAY)

UMGANG MIT MOBILEN GERÄTEN: BITTE BEACHTEN UND REGELN

- **Generelle Sicherheitsmaßnahmen wie Authentifizierung usw.**
  - Mobile Device Management
  - Umgang mit mobilen Speicherträgern (USB, Speicherkarten, Festplatten, ...)
- **Geräteverlust und unautorisierter Zugriff auf das Gerät**
  - Vorbeugende Maßnahmen wie Verschlüsselung
  - Rückwirkende Maßnahmen wie Löschmechanismen
- **Datenverlust**
  - Vorbeugende Maßnahmen wie Backups
  - Rückwirkende Maßnahmen wie Data Recovery
- **Defekte Geräte**
  - Vor Einschicken Daten (sicher) löschen
- **Datenübertragung und Angriff auf die Funkschnittstelle berücksichtigen**
  - VPN
- **Entsorgung**
  - Gelöschte Daten können wieder hergestellt werden
  - Wie ist die Entsorgung alter oder defekter Geräte geregelt?

DATENSCHUTZ IN DER CLOUD

gmds
Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

HEALTHCARE SOLUTIONS

SPEICHERORT DER DATEN

Im Krankenhaus Landesrecht beachten, z.B.:

- Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz - GDSG NRW, zuletzt geändert am 22.02.1994*)

  §7 Abs. (1):

  „Patientendaten sind grundsätzlich in der Einrichtung oder öffentlichen Stelle zu verarbeiten“

* Abgesehen von Änderungen PsychKG (1999, 2005), Anpassungen nach Änderungen SGB V (2005), Überarbeitung Krebsregistergesetz (2005)

SPEICHERORT DER DATEN: DIE „CLOUD“

gmds
Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Dienst	Serverstandort
1. ADrive	1. USA
2. Amazon CloudDrive	2. USA
3. Box	3. USA
4. Dropbox	4. USA
5. Google Drive	5. USA
6. iCloud	6. USA
7. SugarSync	7. USA
8. Telekom Cloud	8. Deutschland
9. Ubuntu one	9. GB
10. Windows Live / SkyDrive	10. Unbekannt (Backup in den USA)
11. Wuala	11. Schweiz, Deutschland, Frankreich

Hinweis: Cloud Computing Sicherheitsempfehlungen des BSI:
https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.htm
https://www.bsi.bund.de/DE/Themen/CloudComputing/Studien/Studien_node.html

KURZER EXKURS: USA UND PATRIOT ACT

- Änderungsgesetz, das mehrere Regelungen des US Code abändert
- Sec. 215 US Patriot Act ändert „Foreign Intelligence Surveillance Act“ (FISA)
- FISA erlaubt Sicherheitsbehörden beim sog. FSI Court eine Anordnung zu beantragen, die eine Person dazu verpflichtet, die bei ihr befindlichen Geschäftsunterlagen herauszugeben
- Patriot Act ermöglicht nun Unterlagen von jeder beliebigen Stelle und bereits unter der Voraussetzung, dass sie mit einer Untersuchung von Terrorismus und Spionage in Verbindung stehen, zu erhalten
- Hinsichtlich der Art der Unterlagen gibt es keine Beschränkungen
- Sec. 505 US erlaubt dem FBI und anderen Justizbehörden, selbst Anordnungen zu erlassen, ohne Zwischenschaltung eines Gerichts
- In Zusammenhang mit FISA kann dem „Datenspender“ auferlegt werden über die Herausgabe der Daten Stillschweigen zu bewahren

PATRIOT ACT UND EUROPA

- Amerikanische Rechtsprechung legt Patriot Act so aus, dass von amerikanischen Gesellschaften auch Daten herausverlangt werden dürfen, die sich im Ausland befinden (Sec. 442(1)(a))
- Die datenschutzrechtliche Lage im betreffenden Ausland wird nicht als einer rechtlichen Herausgabemöglichkeit entgegen stehend betrachtet (Sec. 442(2))
- Steht das Recht des außeramerikanischen Staates der Herausgabe entgegen („blocking statute"), so findet vor dem Erlass einer Herausgabeanordnung eine Abwägung statt (Sec. 442(1)(c))
- In Fällen, in welchen eine Anordnung nach US Patriot Act im Raum steht (Terrorismus, Spionage), dürften die Interessen der USA verstärkt gewichtet und eine Herausgabe als Unumgänglich angesehen werden
- Eine amerikanische Muttergesellschaft kann die Möglichkeit des Zugriffs auf die Unterlagen ihrer ausländischen Tochter nicht absprechen
- Eine amerikanische Tochtergesellschaft kann mittelbar gezwungen werden. Denn eine Nichtbefolgung einer FISA-Anordnung stellt einen sog. contempt of court (Missachtung des Gerichts) dar; Folge: Strafe und Bußgeld

SPEICHERORT DER DATEN: DIE „CLOUD“

Mobile Geräte

- Synchronisation von **Terminen, Kontakten, E-Mails, Fotos usw.**

- Sind Sie sicher, dass in Terminen, Kontakten, Mails usw. keine personenbezogenen Daten enthalten sind?
- Sind Sie sicher, dass keine Patientendaten (z.B. deren Namen) erwähnt werden?
- Ist denn dann ein Vertrag über Auftragsdatenverarbeitung entsprechend §80 SGB X geschlossen worden?
- Bei Serverstandort außerhalb EG: Auftragsdatenvereinbarung geht nicht, nur Funktionsübertragung
  → Es findet eine Übermittlung der Daten statt

– https://www.google.com/intl/de/policies/terms/1

ÜBERMITTLUNG

§5 Abs. (
„... Als Ü
Organis
Organis
Maßnah

Innere, (

➔ Sieh

➔ Was

Betrifft nur NRW?
In 5 Bundesländern ist der Datenaustausch zwischen Abteilungen innerhalb eines Krankenhauses geregelt:

Land	Gesetz
Bremen	BremKHDSG
Hessen	HKHG
Mecklenburg-Vorpommern	LKHG M-V
Nordrhein-Westfalen	GDSG
Saarland	SKHG

FOLGEN EINER ÜBERMITTLUNG

- Schwierig dem Patienten zu verkaufen
- Rechtlich unwirksam: Patient muss informiert einwilligen
  → genaue Aufklärung welche Daten übermittelt werden
- ☠ Unbrauchbare Lösung (Neudeutsch „Bullshit“)

BEI EINSATZ CLOUD UNBEDINGT BEACHTEN:

- Cloud: nicht fragen „wo?“, sondern
  „Brauche ich wirklich eine Cloud?“
  → Kosten-Nutzen-Analyse
- Daten des Krankenhauses werden auf externen Speicherorten nur verschlüsselt abgelegt

FAZIT

1) Mobile Computing sinnvolle Ergänzung vorhandener IT-Arbeitsmittel in der Medizin
2) Einführung ermöglicht
   - flexibles arbeiten
   - Erhebung der Daten am Ort des Entstehens: am Patienten
3) Etablierung einer Richtlinie bzgl. Umgang mit mobile Computing ratsam
4) Abschluß einer Betriebsvereinbarung zum mobile Computing häufig unumgänglich
5) Nutzung von Cloud-Diensten möglich, aber überlegen, ob es wirklich eine Unterstützung ist (Kosten/Nutzen-Analyse) oder ob man nur einem Hype folgt

FRAGEN?

schuetze@medizin-informatik.org

(GPG-Schlüssel auf dem Server abrufbar)