

- Aktuelle Fallbeispiele
- Aktenschrank versus EDV-Archiv
- Szenarien in der IT
- Schutzwürdige Daten: Emails, SocialMedia & Co.
- Rechtliche Grundlagen
- Umsetzung und Evaluation

Wirtschaftlich und politisch motivierte Datendiebstähle:

- 2015/06: Trojaner Bundestag: 2 Jahre Aufarbeitungszeit
- 2014/08: Banking-System PayPal: 1,2 Mio. Passwörter abgegriffen
- 2011/05: Sony: 24,6 Mio. Nutzerkonten mit Kreditkartendaten gestohlen – Schaden: über 10 Mio. USD
- Verfassungsschutz Sachsen: Wirtschaftsspionage CN und RU seit 2011 massiv gestiegen

- Akten durch Brand verloren: Archivierungspflicht vernachlässigt
- PC gestohlen: besonders personenbezogene Daten weitergegeben
- Kontendaten Ihrer Patienten und Mitarbeiter gestohlen → Haftung beim Pflegedienst
- Mitbewerber späht Ihr Management aus
- EDV-Anlage tot: keine Planung und Abrechnung mgl.

- Vorteil: keine unsichtbaren Datendiebstähle
- Prüfen Sie für sich selbst:
 - Zutrittskontrolle zum Archiv
 - Sicherheit der Aktenschränke (Bauart, Schließart)
 - Aufbewahrungsort der Schlüssel
 - Zugangsdokumentation (Logging, Monitoring)
 - Alterungsschutz, Brandschutz
 - Einbruch- und Diebstahlschutz
- Beratung und Prüfung durch Verfassungsschutz

- Vorteil: Platzsparend, Recherche, Verfügbarkeit
- Hohe Kosten für sicheren und redundanten Betrieb
- Datenabgriffe nur mit großem Aufwand erkennbar
- Prüfen Sie für sich selbst:
 - Zugriffsschutz (örtlicher Zugang, Passwörter)
 - Verschlüsselung der Passwörter und Daten
 - Verfügbarkeit (Stromausfall, Internetstörung)
 - Monitoring und Logging

- PC: Booten per CD / USB (Port-Close)
- Datensicherungs-HDD: praktisch auf dem Rechner
- Passwort / Kennwortrichtlinien / Benutzerrechte
- Malware, Spyware & Co.
- Antivirenprogramm und Firewall
- Diebstahlerschwerende Maßnahmen
- Aktualität der Betriebssysteme

Ziel: gestohlener Rechner ist nutzlos, kein Datenverlust da Datensicherung vorhanden

- Zugangs- und Zutrittskontrolle (Rack, Logs)
- Alarmsysteme mit Monitoring
- Keine Hobby-IT: nur professionelle Betreuung!
Risiken bei Servern:
 - gesamte Netzinfrastruktur kann abgerufen werden
 - Missbrauch der Server-Dienste
(Spam-Mails, FTP-Datenhost, ... → rechtliche Konsequenzen)
- Serverimages & Datenbackups regelmäßig zusätzlich extern (Inland) lagern und Datenkonsistenz prüfen

- Smartphones und Tablets sind „Wanzen“ - Bsp. Apple
- GSM Funknetze sind unsicher
- App-Kontrolle: Dauerkommunikation nach Außen
- Beispiele:
 - Class0-SMS: Ortungsdienste (HushSMS)
 - GSM-Antennen: Man-in-the-Middle (13.2. in DD)
 - WIFI: Datenpakete zum mitlesen (zANTI)
 - SpyCam: Abhören und Zuschauen
 - Datenbankverschlüsselung lokal: Bsp. WhatsApp
 - Abtretung der redaktionellen Daten an App-Betreiber

- MITM: sichere PC's schützen nicht vor Datenklau
- Netzwerkdosen, Router: LAN-Kabel anstecken
- Fake-Identität über MAC-Adressen-Clone
- Komfortdienste: UPNP, ARP, DHCP, DNS
- Routerschutz: Herzstück im Netz (Ports, Zugänge)
- Drop-Connection, kein Plain-Traffic, Scans blocken
- WIFI: < WPA2 gleich unverschlüsselt
- **Beispiel: Mikrotik Connection-Log**

Ziel: Router steuert und kontrolliert das Netzwerk

- Fehlermanagement in der EDV
 - Protokollierungs- und Meldepflichten (Tickets)
 - Skills prüfen und weiterbilden (Betriebsblindheit)
- MitarbeiterEinstellung
 - Thematik Umgang mit sensiblen Daten
 - Nutzerrechte-Organigramm einsetzen
 - Verschwiegenheitspflicht in Arbeitsvertrag
- Mitarbeiterentlassung
 - persönliche Zugänge umgehend sperren
 - Email-Adressen umleiten

- Email-Grundlagen: Archivierungspflicht, Signaturpflicht
- Webseiten, Facebook-Sites: Impressumspflicht
- Kommunikation:
 - „CC“-Feld: Klartext-Empfängerliste
 - Schulung der MA: Was darf kommuniziert werden?
 - Webseiten: Vorsichtig vor Abmahnungen (Bilder)
 - WhatsApp-Wunddoku: Einverständniserklärung?
- Imagepflege 2.0: SocialMedia, Firmenblogs
 - Shitstorms, offene Kommunikation: PR-Berater

- BDSG (Bundesdatenschutzgesetz):
 - §4 Abs. 1: Ein Datenschutzbeauftragter ist schriftlich zu bestellen, da...
 - §3 Abs. 9: ...besonders personenbezogene Daten einer Vorabkontrolle unterliegen und muss...
 - §4 Abs. 2: ...die erforderliche Fachkunde der Aufsichtsbehörde nachweisen. Bei Nichteinhaltung...
 - §43 Abs. 3: ...stellt dies eine Ordnungswidrigkeit mit einem Bußgeld bis zu 25.000 EUR dar.

Mindestanforderungen QM

Mindestanforderung QM "Datenschutz in der ambulanten Pflege"

Definition:	<ul style="list-style-type: none"> • Daten zum Gesundheitszustand sind höchst sensible Informationen. Der Gesetzgeber hat daher den Schutz dieser Daten durch zahlreiche Gesetze und Verordnungen reglementiert. • Mit Abschluss des Pflegevertrages stimmt der Patient der Erhebung, der Speicherung, der Verarbeitung und ggf. der Übermittlung seiner Daten durch den Pflegedienst zu. Wir dürfen die Daten im Rahmen der Pflege sowie für die Abrechnung unserer Leistungen nutzen. • Der Missbrauch von Daten kann mit Geldbußen von bis zu 25.000 € pro Verstoß geahndet werden. 	
Grundsätze:	<ul style="list-style-type: none"> • Das Vertrauen des Patienten in die Sicherheit und Vertraulichkeit seiner Daten ist ein Eckpfeiler jeder konstruktiven Kooperation mit dem Pflegedienst. • Die sorgfältige Verwaltung und Nutzung persönlicher Daten ist für uns eine Selbstverständlichkeit. Wir begrüßen daher die restriktive Gesetzgebung zum Datenschutz. 	
Ziele:	<ul style="list-style-type: none"> • Das Vertrauensverhältnis zwischen Patient und Pflegedienst wird geschützt. • Alle gesetzlichen Vorgaben werden erfüllt. Insbesondere wird das informationelle Selbstbestimmungsrecht jedes Patienten beachtet. • Kein unberechtigter Dritter erhält Zugriff auf sensible Informationen. Dieses unabhängig davon, ob die Daten digital auf einem Computer gespeichert sind, gedruckt wurden oder handschriftlich vermerkt sind. 	
Vorbereitung:	<ul style="list-style-type: none"> • Im Erstgespräch mit dem neuen Patienten informieren wir diesen zum Thema Datenschutz. • Alle Mitarbeiter werden in regelmäßigen Abständen zum Thema Datenschutz weitergebildet. • Es wird ein Datenschutzbeauftragter benannt. • Alle Mitarbeiter werden arbeitsvertraglich zur Einhaltung des Datenschutzes angehalten. • Wenn eine Pflegekraft den Verdacht hat, dass unberechtigte Dritte Zugriff auf sensible Daten hatten, werden umgehend die Pflegedienstleitung und der Datenschutzbeauftragte informiert. 	
Durchführung:	Computer	<p>Auf unseren Computern sind zahlreiche sensible Datensätze gespeichert. Diese schützen wir durch verschiedene Maßnahmen:</p> <ul style="list-style-type: none"> • Der Raum, in dem die Computer stehen, ist durch ein zusätzliches Schloss gesichert. Wenn der Pflegestützpunkt nicht besetzt ist, wird der Raum abgeschlossen. • Externe Speichermedien wie etwa mobile Festplatten, gebrannte DVDs usw. werden in einem Schrank gelagert. Der Schrank wird verschlossen. Wann immer möglich werden mobile Laufwerke komplett verschlüsselt, etwa durch die Nutzung der kostenlosen Software "TrueCrypt".

		<ul style="list-style-type: none">• Der Zugriff wird beschränkt. Jeder Mitarbeiter, zu dessen Aufgaben die Bedienung des Computers zählt, erhält einen eigenen Benutzernamen und ein Passwort. Dieses darf er nicht an Dritte weitergeben.• Wir nutzen stets Computer mit zwei eingebauten Festplatten. Ein Laufwerk enthält das Betriebssystem und die notwendigen Anwendungsprogramme. Ein zweites Laufwerk speichert die zu schützenden Daten. (Hinweis: Diese Spezifikation sollte dem Computer-Händler schon vor dem Kauf genannt werden. Die Gehäuse beider Festplatten im Computergehäuse werden von ihm per Aufkleber entsprechend mit "Windows" bzw. "Daten" beschriftet. Die Nutzung einer Festplatte mit zwei getrennten Partitionen ist keine Alternative.)• Bei Defekten an der Hardware unseres Computersystems bevorzugen wir eine Reparatur vor Ort unter Aufsicht durch einen Mitarbeiter. Falls ein Computer in einer Werkstatt repariert werden muss, wird zuvor das Laufwerk mit den sensiblen Daten entfernt und im Pflegestützpunkt verschlossen. Die Festplatte mit dem Betriebssystem verbleibt im Computer. (Alternative: Verschlüsselung auch der internen zweiten Festplatte.)• Wir achten darauf, dass bei einem Datentransfer (etwa zu einem Abrechnungsdienstleister) keine Informationen an Unbefugte gelangen. Daher gibt es nur folgende Optionen:<ul style="list-style-type: none">○ Transfer per Internet über eine gesicherte (verschlüsselte) Leitung○ Transfer per Post als verschlüsselte DVD○ eigenhändiger Transport mit persönlicher Übergabe, dieses ggf. auch als unverschlüsselter Datenträger• Das Betriebssystem des Computers wird per Auto-Update stets auf dem neusten Stand gehalten. Der Virenschutz wird täglich aktualisiert. Bei Verdacht auf eine Vireninfektion wird der Computer ausgeschaltet. Der Mitarbeiter ruft dann unverzüglich einen Techniker.• Wir nutzen in unserem Pflegestützpunkt ein WLAN-Netzwerk. Wir stellen sicher, dass jedes Gerät die Verschlüsselungsmethode WPA2 nutzt. Die Verwendung von WPA ist unsicher.• Alternativtext: Wir nutzen in unserem Pflegestützpunkt kein WLAN, sondern ein kabelgestütztes Netzwerk. Wenn einzelne Komponenten (z.B. der DSL-Router) eine WLAN-Funktion haben, so wird diese Option abgeschaltet.• Wenn das Büro in einem Bereich mit Besucherverkehr liegt, treffen wir zusätzliche Vorkehrungen zum Schutz der Daten:<ul style="list-style-type: none">○ Der Computer wird mit einem Bildschirmschoner ausgestattet, der sich nach einer Minute Inaktivität einschaltet.○ Wenn ein Mitarbeiter den Computer verlässt, so muss die jeweilige Anwendung geschlossen werden. Dieses gilt insbesondere für die Pflegedokumentationssoftware.
	Plantafeln	<ul style="list-style-type: none">• Plantafeln, auf denen die Namen von Patienten vermerkt sind, werden vor unerwünschten Einblicken geschützt. Sie dürfen in keinen Räumen stehen, in denen sie von außen etwa durch ein Fenster einsehbar sind.• Falls möglich werden die Plantafeln durch ein Rollo oder eine klappbare Deckwand geschützt. Wenn die Plantafel mit Rollen ausgestattet ist, wird diese zur Wand gedreht.• Eine Plantafel sollte in einem Raum stehen, der für Besucher nicht zugänglich ist.

Mindestanforderungen QM



	<p>Datenschutz beim Transport</p>	<ul style="list-style-type: none"> • Unterlagen werden außerhalb des Pflegestützpunktes stets in undurchsichtigen Schutzhüllen transportiert, i.d.R. also in Mappen, Ordnern usw. • Sensible Kundendaten werden nicht offen im Auto gelagert, etwa auf dem Beifahrersitz. Dieses gilt insbesondere für die Leistungsnachweise und Protokolle (Erstgespräch, Pflegevisite usw.). Derartige Dokumente werden mit in die Wohnung des Patienten genommen. Alternativ können diese in einer Schließbox im Auto gelagert werden, wenn dieser Behälter fest mit der Karosserie verbunden ist. • Wenn Dokumente mit in den Haushalt des Patienten genommen werden, werden diese auch dort vor unberechtigter Einsichtnahme geschützt. Die Pflegekraft nimmt die Dokumente stets in den Raum mit, in dem sie die Pflegemaßnahmen durchführt.
	<p>Weiteres</p>	<ul style="list-style-type: none"> • Es ist weiterhin darauf zu achten, dass patientenbezogene Unterlagen nicht öffentlich zugänglich, z.B. auf Schreibtischen herumliegen. Sie sind sofort in die Dokumentationen einzuordnen. • Wir stellen sicher, dass eingehende Faxe vor den Blicken von Unbefugten geschützt sind.
<p>Nachbereitung:</p>		<ul style="list-style-type: none"> • Verschiedene Faktoren können dazu führen, dass wir auch vertrauliche Daten an staatliche Stellen weitergeben müssen, etwa <ul style="list-style-type: none"> ◦ wenn der Bewohner eine Straftat nach § 138 StGB plant ◦ wenn die öffentliche Gesundheit durch Infektionskrankheiten bedroht ist • Probleme bei der Handhabung des Datenschutzes werden regelmäßig bei Teambesprechungen sowie im Qualitätszirkel thematisiert.
<p>Dokumente:</p>	<p>-</p>	
<p>Verantwortlichkeit / Qualifikation:</p>		<ul style="list-style-type: none"> • alle Mitarbeiter

- Bestellung eines Datenschutzbeauftragten
- IST-Analyse der Infrastruktur (anhand der Beispiele)
- SOLL-Konzept nach Schwachstellenanalyse definieren
- Umsetzung und halbjährige Prüfung der Ziele
- Weiterbildungen des Datenschutzbeauftragten
- Dokumentation der geleisteten Bemühungen den Normen des BDSG gerecht zu werden im Falle eines Datendiebstahls
- Meldepflichten bei Datendiebstählen einhalten

- CareSocial führt Security-Audits durch
 - Objektbegehung mit simuliertem Datendiebstahl
 - Topologieplan mit Schwachstellenanalyse
 - SOLL-Konzept zur Abdichtung der Angriffspunkte
 - Umsetzung und Betreuung sensibler Infrastruktur
- CareSocial bietet zertifizierte Schulungen zum Thema Datenschutz und Datensicherheit an

Vielen Dank für Ihre Aufmerksamkeit!

CareSocial GmbH

Johannes Kersten
Geschäftsführung

Gostritzer Straße 61-63
01217 Dresden
0351 / 26443-100
office@caresocial.de

Download des Scripts unter

www.caresocial.de/datenschutz.pdf



Care Social

Software für ambulante Pflegedienste

www.caresocial.de



Care Factoring

Abrechnungszentrum mit Vorfinanzierung

www.carefactoring.de



Care Intense

Software für Intensivpflegedienste

www.careintense.de



Care Smart

Mobile Datenerfassung für Pflegedienste

www.caresmart.de