Mitarbeiterinformation Datenschutz im Krankenhaus

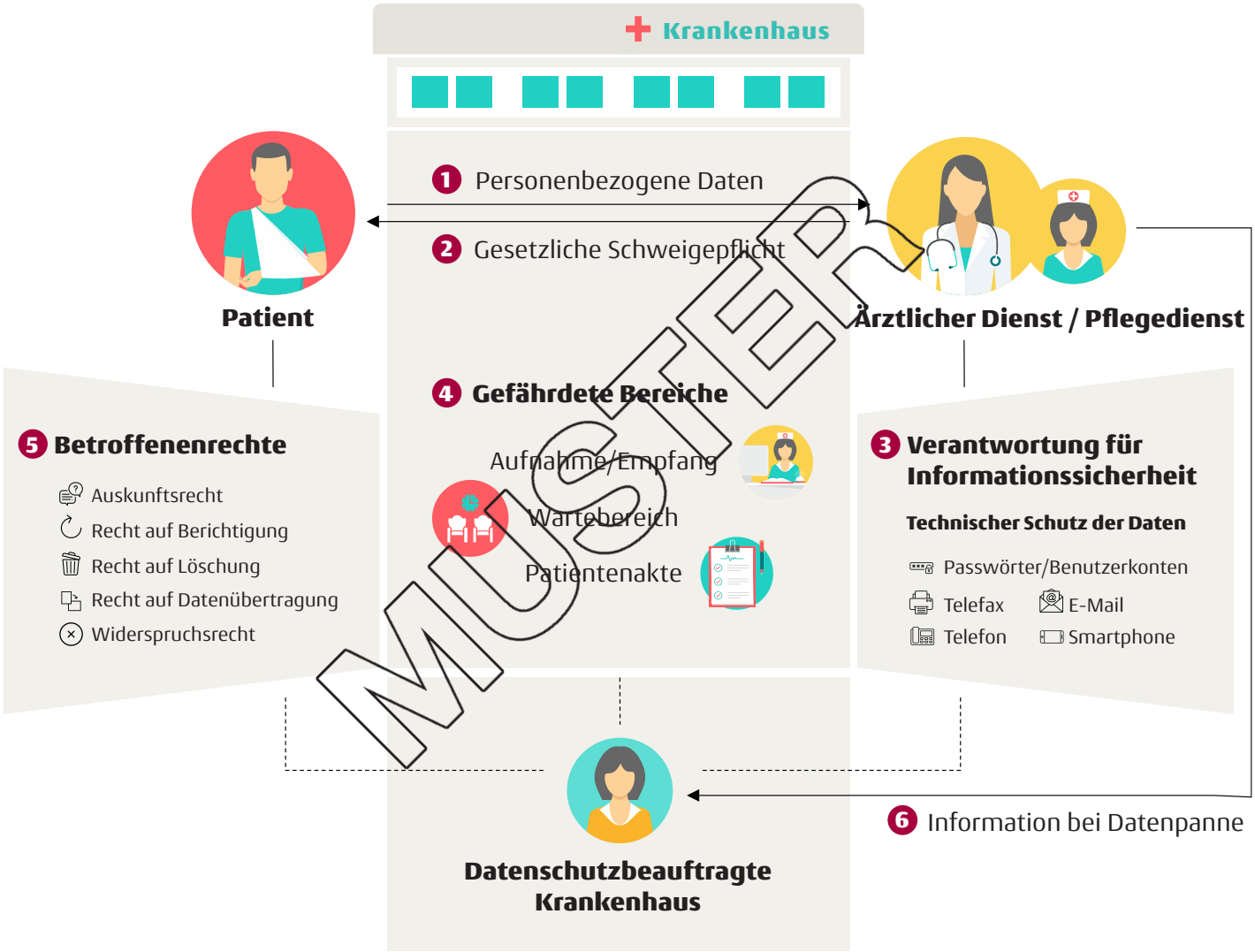
Merkblatt für Beschäftigte

Krankenhaus-IT JOURNAL

DATAKONTEXT

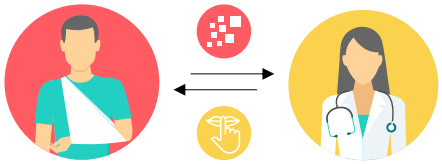
Inhalt

1 Überblick Datenschutz im Krankenhaus



2 Einführung

Das Verhältnis von Arzt und Patient ist durch das Vertrauen geprägt, das der Patient dem Arzt entgegenbringt. Der Patient offenbart seinem Arzt persönlichste Dinge. Das Vertrauen des Patienten setzt die Verschwiegenheit des Arztes voraus.



So enthält bereits der hippokratische Eid eine erste medizinische Datenschutzregel:

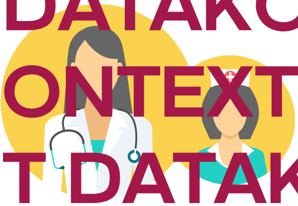
Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten.[1]

Diese ärztliche Schweigepflicht findet ihren Niederschlag auch in § 203 des Strafgesetzbuches (StGB). § 203 StGB stellt es unter Strafe, wenn Ärzte und ärztliche Hilfspersonen die Schweigepflicht verletzen, indem sie unzulässigerweise vertrauliche Informationen, die ihnen als Arzt anvertraut oder bekannt geworden sind, offenbaren.

Die europäische Datenschutz-Grundverordnung (DSGVO) zählt Gesundheitsdaten zu den besonders sensiblen personenbezogenen Daten, deren Verarbeitung nur unter sehr engen Voraussetzungen zulässig ist und die besonders geschützt werden müssen.

1 https://de.wikipedia.org/wiki/Eid_des_Hippokrates#Wortlaut

2.1 Gesetzliche Schweigepflicht



Das medizinische Personal und die Angestellten in der Verwaltung des Krankenhauses unterliegen der gesetzlichen Schweigepflicht gemäß § 203 Strafgesetzbuch (StGB).

Bitte beachten Sie, dass die Gleichstellungsvorschrift des § 203 Abs. 3 StGB den Täterkreis um „Gehilfen" des Arztes erweitert. Berufsmäßig tätige Gehilfen sind zum Beispiel die Mitarbeiter der Krankenhausverwaltung oder das technische Bedienungspersonal von medizinischen Geräten. Auch Auszubildende im Krankenhaus unterliegen der Schweigepflicht.

Gemäß § 203 Strafgesetzbuch dürfen keine Geheimnisse von Patienten offenbart werden. Dabei ist sowohl der medizinische als auch der private Bereich der Patienten geschützt.

Ein Geheimnis ist jede Tatsache, die nur einem begrenzten Personenkreis bekannt ist und an deren Geheimhaltung der Patient ein schutzwürdiges Interesse hat. Davon sind neben Informationen zur Gesundheit auch andere private Informationen über den Patienten zu verstehen (zum Beispiel: finanzielle Probleme, Eheprobleme). Auch sogenannte „Drittgeheimnisse", also Geheimnisse, die Personen aus dem Verwandten- und Bekanntenkreis des Patienten betreffen, werden von der Schweigepflicht erfasst, wenn der Patient an der Geheimhaltung ein schutzwürdiges Interesse hat (zum Beispiel Alkoholprobleme des Lebensgefährten eines Patienten).

Die Schweigepflicht gilt gegenüber jeder Person, die nicht unmittelbar an der medizinischen Betreuung des Patienten beteiligt ist. Das gilt also insbesondere für Kolleginnen und Kollegen, die nicht in die Behandlung des Patienten eingebunden sind.

Die gesetzliche Schweigepflicht wirkt auch nach dem Tod der betroffenen Person weiter.

Es ist darauf zu achten, dass bei Visiten oder Gesprächen auf dem Flur die Vertraulichkeit angemessen gewährleistet wird.

Spricht der Patient im Mehrbettzimmer das medizinische Personal wegen eines bestimmten Themas an, obwohl er weiß, dass andere Patienten mithören können, kann davon ausgegangen werden, dass er an der Geheimhaltung des Gesprächsinhalts kein Interesse hat.

Im Rahmen des Wissensaustausches unter Kolleginnen und Kollegen muss darauf geachtet werden, dass mit Hilfe der weitergegebenen Informationen eine Identifizierung des Patienten nicht möglich ist.

Beispiele

Die Schweigepflicht besteht auch gegenüber dem Hausarzt des Patienten, wenn dieser nicht in die Behandlung eingebunden ist.

Bettbeschriftungen am Patientenbett, auf denen Personalien, Religionszugehörigkeit, Informationen zur Medikation und andere persönliche Daten des Patienten genannt werden, stellen einen Verstoß gegen die Schweigepflicht dar.

Wenn der OP-Plan, in dem Namen von Patienten und die Art des Eingriffs festgehalten ist, in einem Flur hängt, zu dem auch Besucher des Krankenhauses Zugang haben, dann ist das ein klarer Verstoß gegen die Schweigepflicht.

Es dürfen keine Auskünfte über den Gesundheitszustand eines Patienten an dessen Ehepartner gegeben werden. Dies ist nur dann möglich, wenn eine ausdrückliche Einwilligung des Patienten vorliegt. Liegt keine Einwilligung vor, dann sollte man anfragende Angehörige bitten, sich die Informationen direkt bei dem Patienten zu holen.

3 Informationssicherheit

3.1 Datenschutz und IT-Sicherheit

Beim Datenschutz geht es darum, den Patienten davor zu schützen, dass sein Persönlichkeitsrecht durch die missbräuchliche Verwendung seiner personenbezogenen Daten verletzt wird.

Das Bundesverfassungsgericht hat im Volkszählungsurteil von 1983 das „Recht auf informationelle Selbstbestimmung“ entwickelt. Dieses Recht lässt sich sehr prägnant mit dem Satz „Ich entscheide, wer was über mich weiß“ zusammenfassen.

Der technische Schutz der Daten durch Maßnahmen der IT-Sicherheit ist eine zwingende Voraussetzung, damit die Persönlichkeitsrechte der Patienten wirksam geschützt werden können.

Die klassischen Schutzziele der IT-Sicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit.

Vertraulichkeit

Nur derjenige, der die Daten im Rahmen seiner Tätigkeit benötigt, hat Zugriff auf die Daten. Das wird insbesondere durch ein detailliertes Benutzer- und Zugriffskonzept erreicht.

Integrität

Es muss technisch gewährleistet werden, dass Daten nicht verfälscht werden können. Um das zu erreichen, wird zum Beispiel protokolliert, wer wann welche Daten geändert hat.

Verfügbarkeit

Es muss sichergestellt sein, dass der Zugriff auf die Daten jederzeit möglich ist. Ein wichtiges Mittel, um die Datenverfügbarkeit sicherzustellen, ist das regelmäßige Anfertigen einer Sicherheitskopie („Backup“), so dass die Daten im Falle eines Datenverlusts schnell wieder hergestellt werden können.

3.2 Passwörter und Benutzerkonten

Passwörter sollten mindestens 12 Zeichen lang sein. Sie machen es potenziellen Angreifern deutlich schwerer, Ihr Passwort zu „knacken“, wenn Sie im Passwort Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen verwenden.

Verwenden Sie für Passwörter niemals Wörter, die im Wörterbuch zu finden sind.

Dienstliche Smartphones sollte mindestens mit einer 6-stelligen PIN gesichert werden. Alternativ kann auch ein Sperrmuster verwendet werden. Auf freiwilliger Basis können auch biometrische Merkmale wie Fingerabdruck und Gesichtserkennung zur Anmeldung genutzt werden.

Passwörter und Zugangsdaten, die nicht mehr geheim sind, sollten sofort geändert werden, da sie keinerlei Schutz bieten.

Für unterschiedliche Dienste und Anwendungen sollten unterschiedliche Passwörter verwendet werden. Bitte verwenden Sie auch keine ähnlichen Passwörter für unterschiedliche Dienste und Anwendungen.

Sie machen es potenziellen Angreifern deutlich schwerer auf Ihr Gerät zuzugreifen, wenn Sie eine sogenannte Zwei-Faktor-Authentifizierung wählen. Sie benötigen dann zum Beispiel sowohl eine PIN (Faktor Wissen), als auch einen Fingerabdruck (Faktor biometrisches Merkmal), um das Smartphone zu entsperren. Bitte nutzen Sie die Zwei-Faktor-Authentifizierung, wo immer das möglich ist.

Benutzerkonten sind Ihre Zugangsdaten für ein System. Benutzerkonten dürfen nicht geteilt, sondern immer nur von einer Person genutzt werden.

Beachten Sie interne Vorgaben. Insbesondere Hinweise und Regelungen zur Datensicherheit garantieren den Schutz der Daten.

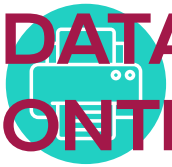
Top Ten deutscher Passwörter 2021

1. 123456
2. passwort
3. 12345
4. hallo
5. 123456789
6. qwertz
7. schatz
8. basteln
9. berlin
10. 12345678

Quelle: Hasso-Plattner-Institut an der Universität Potsdam

Solche leicht zu erratenden Passwörter sollten Sie keinesfalls verwenden!

3.3 Telefax



Bis vor einigen Jahren galt ein Telefax als sichere Methode, um auch sensible personenbezogene Daten, wie Gesundheitsdaten, zu übermitteln. Durch technische Änderungen in den Telefonnetzen hat sich das grundlegend geändert.

Faxe werden nicht mehr leitungsvermittelt, sondern paketvermittelt über das Internet übertragen. Aufgrund dieser technischen Veränderung hat ein Fax hinsichtlich der Vertraulichkeit das gleiche niedrige Sicherheitsniveau wie eine unverschlüsselte E-Mail.

Für den Versand personenbezogener Daten müssen daher alternative, sichere und geeignete Verfahren genutzt werden. Das können zum Beispiel Ende-zu-Ende-verschlüsselte E-Mails oder Briefpost sein.

3.4 Telefon

Bitte achten Sie beim Telefonieren darauf, dass keine unbefugten Personen das Gespräch mithören können.

Lässt es sich nicht vermeiden, dass Unbefugte mithören, vermeiden Sie es Namen zu nennen oder sensible Einzelheiten zu erwähnen.

Sensible Informationen sollten nur dann herausgegeben werden, wenn man sich der Identität des Gesprächspartners sicher sein kann. Im Zweifel rufen Sie die anfragende Stelle bitte zurück.

Deaktivieren Sie die Wahlwiederholung, insbesondere dann, wenn das Telefon für Besucher oder Patienten zugänglich ist.

3.5 E-Mail

Beim Versand sensibler Daten per E-Mail über das Internet muss darauf geachtet werden, dass diese Daten immer verschlüsselt versendet werden.

Beachten Sie, dass auch bei einer verschlüsselten E-Mail die Betreffzeile unverschlüsselt übermittelt wird. Nennen Sie also keine Namen und andere sensible Informationen im Betreff der E-Mail.

E-Mail-Anhänge können Schadsoftware enthalten. Behandeln Sie E-Mail-Anhänge daher mit großer Vorsicht.

Verwenden Sie für Rundschreiben mit großem Verteiler die BCC-Funktion (Blind Copy).

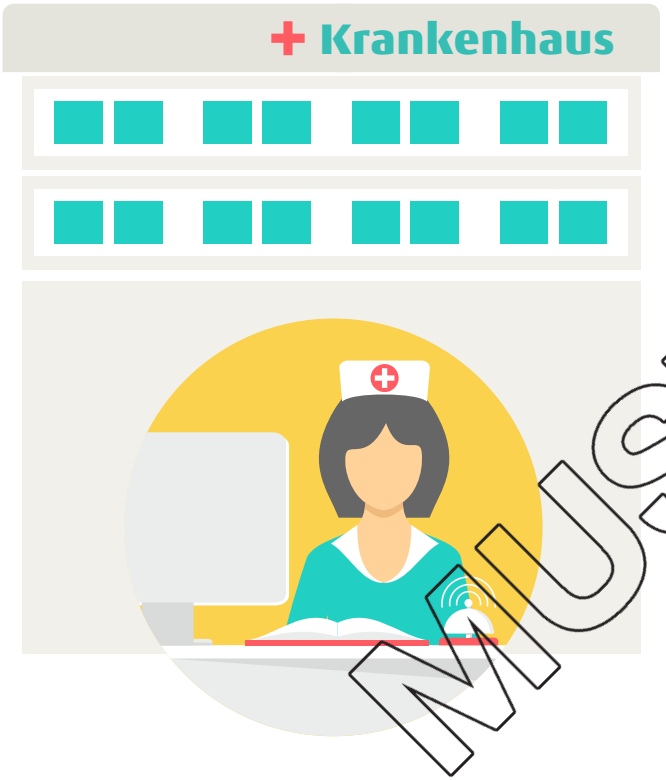
3.6 Smartphone

Nutzen Sie Ihr privates Smartphone nicht für dienstliche Zwecke.

Apps und Dienste, die Sie privat nutzen, dürfen nicht verwendet werden, um Patientendaten zu verarbeiten. Darunter fallen zum Beispiel Messenger wie WhatsApp oder Telegram sowie Cloud-Speicher etwa wie Dropbox oder Google Drive.

4 Datenschutz in der Praxis

4.1 Aufnahme/Empfang



Die Erfassung der Patientendaten beginnt in der Regel bei der Aufnahme. Dabei muss das Gebot der Datensparsamkeit beachtet werden. Es dürfen also nur solche Daten erhoben werden, die für die Behandlung und die Abrechnung benötigt werden.

- Bei der administrativen Aufnahme sind dies Name, Anschrift, Geburtsdatum und Angaben über die Krankenversicherung.
- Weitere Angaben, z.B. zur Religionszugehörigkeit, zum Familienstand etc., können zusätzlich als „freiwillige Angaben" abgefragt werden.

Bei der Aufnahme wird dem Patienten der Behandlungsvertrag ausgehändigt und seine Einwilligung zur Weitergabe von Daten z.B. an den Hausarzt, die Krankenhausseelsorge und weitere Stellen eingeholt.

Bei dauerhaft nicht einwilligungsfähigen Patienten muss der Behandlungsvertrag einer entsprechend bevollmächtigten Person/Betreuer ausgehändigt werden.

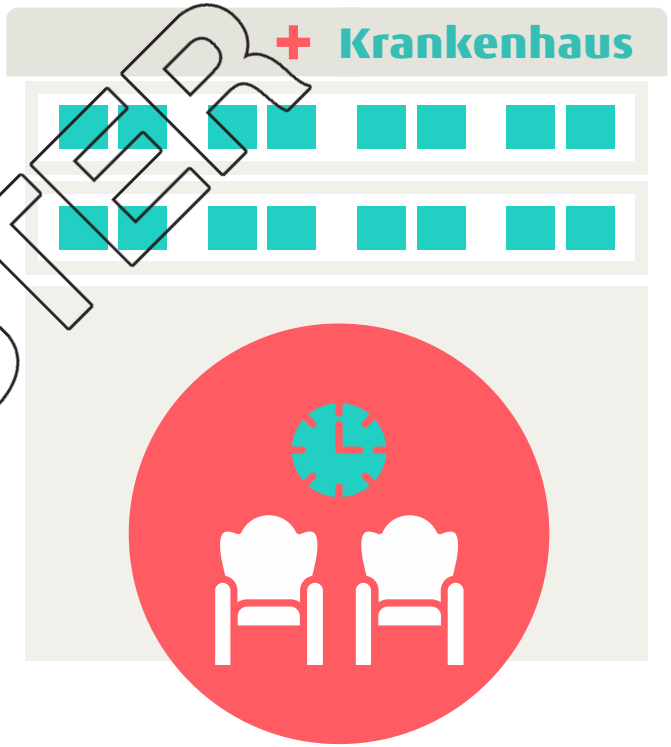
Werden Patienten in der Notaufnahme eingeliefert, kann die Datenverarbeitung aufgrund der Sonderregelung in Artikel 9 Absatz 2 lit. c DS-GVO erfolgen. Die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich und diese ist außerstande, ihre Einwilligung zu geben.

4.2 Wartebereiche

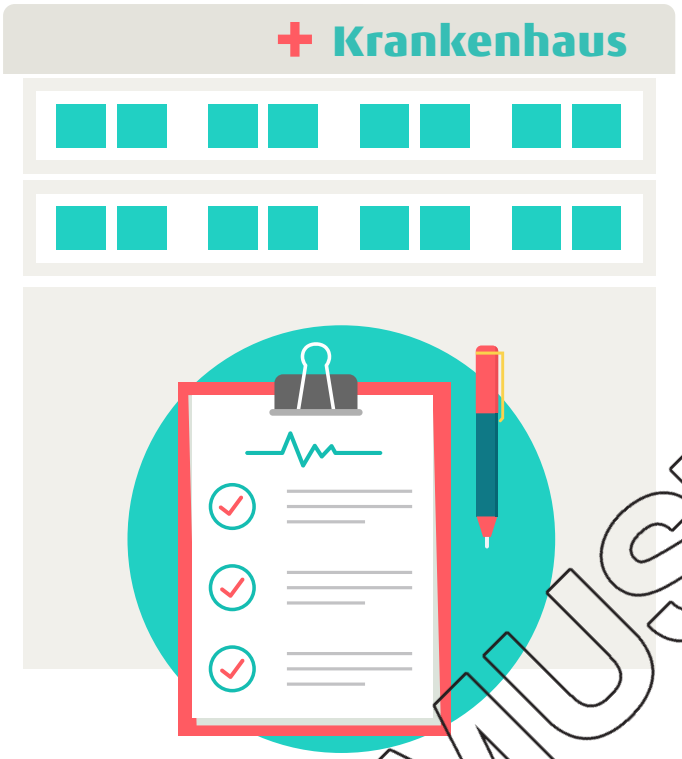
Überall dort, wo Publikumsverkehr herrscht – sei es bei der Aufnahme, auf der Station oder vor Behandlungsräumen – besteht die Gefahr, dass sensible Patientendaten von Unbefugten zur Kenntnis genommen werden.

Um die nötige Diskretion zu wahren, sollte in diesen gefährdeten Bereichen daher darauf geachtet werden, dass

- vorhandene Türen zu Wartebereichen geschlossen bleiben,
- wartende Patienten und Besucher keine Gespräche mit anhören können,
- Patienten, die aufgerufen werden, so angesprochen werden, dass andere Anwesende nicht erfahren, worum es sich im Einzelnen handelt,
- Computermonitore nicht einsehbar sind und der passwortgeschützte Bildschirmschoner aktiviert ist,
- Akten und Dokumente nicht unbeaufsichtigt bzw. für Unbefugte zugänglich abgelegt werden.



4.3 Umgang mit Patientenakten



Die Patientenakte, sowohl in Papierform als auch in einer digitalen Variante, umfasst alle über den Patienten gesammelten Informationen: Identifikationsdaten, administrative Daten, medizinische Daten. Auch hier steht die Vermeidung einer unbefugten Offenbarung im Vordergrund.

Generell muss der Umgang mit Dokumenten in einer Art und Weise erfolgen, dass eine unbefugte Offenbarung, sprich die Einsichtnahme durch Unbefugte, ausgeschlossen ist.

- Akten müssen so abgelegt werden, dass Besucher oder Patienten keinen Einblick nehmen können.
- Akten dürfen nicht unbeaufsichtigt offen liegen gelassen werden.
- Akten müssen in verschließbaren Räumen oder Möbelstücken verwahrt werden.
- Es darf nie die komplette Akte, sondern nur die zur Erfüllung der jeweiligen Aufgabe notwendigen Teile (Behandlung oder Abrechnung) weitergegeben werden.

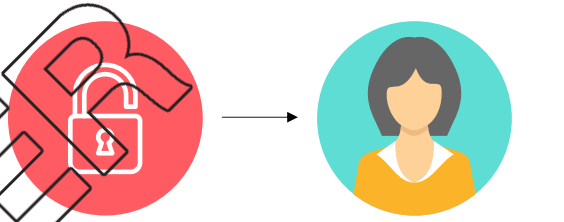
- Dokumente, die in die Akte aufgenommen werden, müssen auf Korrektheit und Vollständigkeit geprüft werden.
- Nach der Behandlung muss die Akte gesperrt werden, bzw. der Zugriff darf nur einem eingeschränkten Personenkreis möglich sein.
- Außerdem gilt es zu beachten, dass die Mitnahme von Akten aus dem Krankenhaus grundsätzlich untersagt und nur in Ausnahmefällen erlaubt ist.

4.4 Datenpanne

Der Verlust von Dokumenten mit personenbezogenen Daten oder die Offenbarung von Gesundheitsdaten gegenüber Unberechtigten, muss gemäß Artikel 33 Datenschutz-Grundverordnung der Aufsichtsbehörde gemeldet werden, wenn ein **Risiko** für die Rechte und Freiheiten natürlicher Personen besteht.

Besteht ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen, müssen zusätzlich alle betroffenen Personen gemäß Artikel 34 Datenschutz-Grundvorordnung informiert werden.

Ob ein Risiko oder gar ein hohes Risiko besteht, beurteilt die Datenschutzbeauftragte oder der Datenschutzbeauftragte der Einrichtung. Die Meldung an die Datenschutz-Aufsichtsbehörde muss innerhalb von **72 Stunden** erfolgen. Bitte informieren Sie daher sofort die Datenschutzbeauftragte oder den Datenschutzbeauftragten, wenn es zu einer Datenpanne gekommen ist.



4.5 Beschäftigte als Patienten

Gesundheitsdaten von Beschäftigten als Patient sind oftmals besonders sensibel zu würdigen. Es muss dafür gesorgt werden, dass nur die zuständigen Beschäftigten Kenntnis haben. Keinesfalls dürfen die Informationen über die Krankheit im Zusammenhang mit den Informationen über das Arbeitsverhältnis zusammengeführt und gemeinsam verarbeitet werden. Oftmals kann die Patientenakte im Krankenhausinformationssystem versiegelt werden. Informieren Sie sich über die technischen Möglichkeiten in Ihrem KIS.

5 Der gesetzliche Rahmen

Im Krankenhaus kommt einerseits das Strafgesetzbuch zur Anwendung. Andererseits müssen die Datenschutzgesetzgebung und weitere im Krankenhaus relevante Gesetze beachtet werden.

Den Kernbereich bilden hierbei (nicht abschließend):

- StGB (Strafgesetzbuch)
- StPO (Strafprozessordnung)
- BGB (Bürgerliches Gesetzbuch)
- DSGVO (EU-Datenschutz-Grundverordnung)
- BDSG (Bundesdatenschutzgesetz)
- Landeskrankenhausgesetze

Im Rahmen der Behandlung werden ggf. folgende Gesetze zu berücksichtigen sein:

- Arzneimittelgesetz
- Betäubungsmittelgesetz
- Gendiagnostikgesetz
- Infektionsschutzgesetz
- Transplantationsgesetz

Länderspezifische Gesetze sind zum Beispiel

- die LDSG (Landesdatenschutzgesetze)
- Bestattungsgesetze der Länder
- Krebsregistergesetze der Länder

Bei Krankenhäusern in öffentlicher und privater Trägerschaft gilt grundsätzlich die Datenschutz-Grundverordnung (DSGVO). Weitere relevante Regelungen können für nicht-öffentliche Träger im Bundesdatenschutzgesetz (BDSG) und für öffentliche Träger in den Landesdatenschutzgesetzen (LDSG) vorhanden sein.

In den konfessionellen Häusern wird der Datenschutz grundsätzlich durch die konfessionellen Datenschutzgesetze geregelt.

Relevant sind hier:

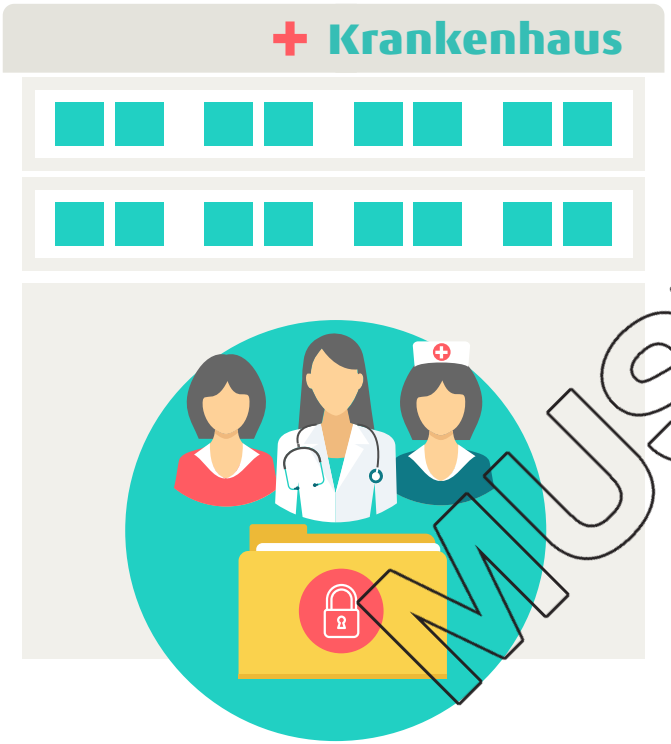
- das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) und
- das Gesetz über den Kirchlichen Datenschutz (KDG) für die katholische Kirche.

Auch die Sozialgesetzbücher (I, V, VII, IX, X; XI) sind wichtig. Sie enthalten zum Beispiel Regelungen für den Datentransfer zwischen Leistungsträgern und Leistungserbringern im Rahmen der Abrechnung von Behandlungen.

Das „Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten“ (Patientenrechtegesetz, PatRG) wirkt sich auf eine Reihe von relevanten gesetzlichen Regelungen aus. Im BGB sind das die Regelungen zum Behandlungsvertrag (§§ 630a bis 630h).

5.1 Verantwortung für den Datenschutz

Nach dem Standes- und Strafrecht sind sehr viele Mitarbeiter im Krankenhaus persönlich für die Wahrung der Schweigepflicht verantwortlich. Organisatorisch werden dazu oftmals von der Betriebsleitung Regelungen formuliert und im Qualitätsmanagement bekannt gegeben.



Gemäß § 203 des Strafgesetzbuches kann die unbefugte Offenbarung von Geheimnissen (des Patienten), die dem Arzt beruflich bekannt geworden sind, sogar mit einer Freiheitsstrafe geahndet werden. Gemäß dem Datenschutzrecht ist der „für die Verarbeitung Verantwortliche" für den Datenschutz zuständig. Dieser „für die Verarbeitung Verantwortliche" ist der juristische Träger der Einrichtung, also z.B. eine GmbH oder eine andere Gesellschaft.

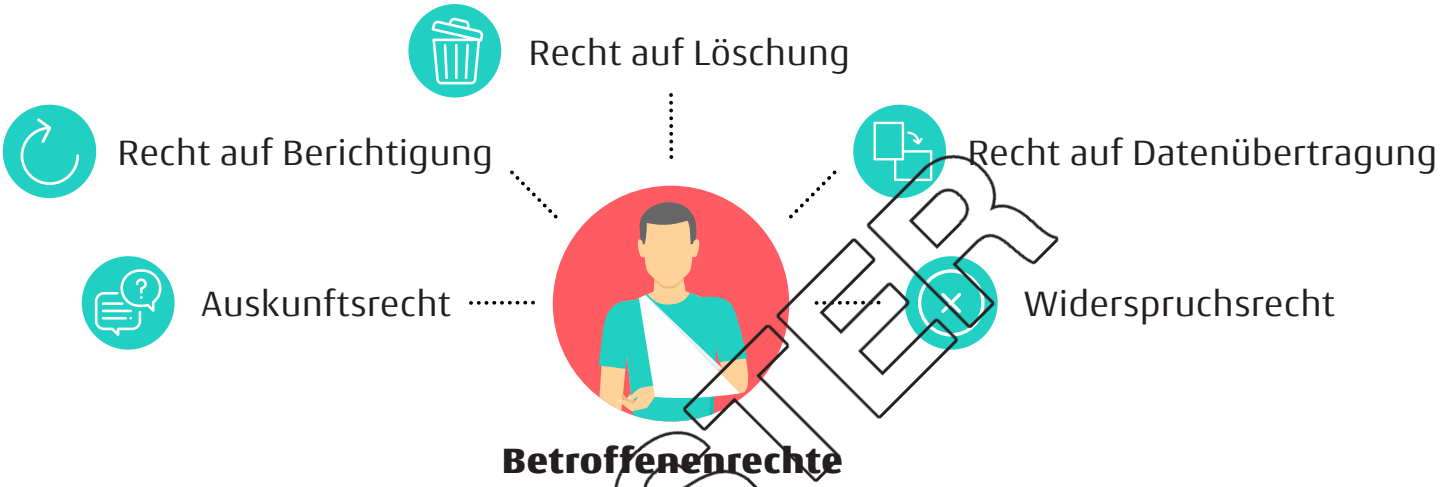
In einer Gemeinschaftspraxis sind die dort arbeitenden Ärzte Teil eines Behandlungsteams. Hier ist die Gesellschaft, welche die Ärzte gebildet haben, für den Datenschutz verantwortlich. Der jeweilige Arzt trägt die Verantwortung für die Einhaltung der Schweigepflicht.

Ärzte mit einer persönlichen Ermächtigung und Belegärzte nutzen (bei Versorgung von Privatpatienten) die Infrastruktur des Krankenhauses, tragen aber für ihren jeweiligen Bereich selbst die Verantwortung für die Schweigepflicht. Dabei sind Angestellte des Krankenhauses, die für sie tätig sind, ihre „Gehilfen".

Alle Mitarbeiter des Krankenhauses, die mit Patientendaten umgehen, sind weisungsgebundene Erfüllungsgehilfen des behandelnden Arztes. Diese „Gehilfen" unterliegen der gesetzlichen Schweigepflicht.

Keine Gehilfen im Sinne von § 203 Absatz 3 Strafgesetzbuch sind Hausmeister, Handwerker sowie das Küchen- und Reinigungspersonal. Diese Berufsgruppen unterliegen nicht der gesetzlichen Schweigepflicht.

5.2 Betroffenenrechte



Personen, deren Daten verarbeitet werden, haben insbesondere folgende Rechte:

- Recht auf Auskunft
- Recht auf Löschung
- Recht auf Berichtigung von falschen Daten
- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht gegen Werbung

Wenn Sie eine entsprechende Anfrage von Patienten (auch Mitarbeitern) erhalten, dann sprechen Sie bitte umgehend mit der Datenschutzbeauftragten oder dem Datenschutzbeauftragten ihrer Einrichtung. Nur so kann sichergestellt werden, dass die Anfrage gesetzeskonform beantwortet wird. Teilen Sie der anfragenden Person lediglich mit, dass Sie die Anfrage umgehend weiterleiten werden.

6 Quellen

Die Schweigepflicht des Pflegepersonals, RA Robert Roßbruch
(abrufbar unter https://www.htwsaar.de/sowi/fakultaet/personen/professoren/prof-dr-robert-rossbruch/veroffentlichungen/schweigepflicht.pdf)

Telefax ist nicht Datenschutz konform, Orientierungshilfe der bremischen Landesbeauftragten für Datenschutz
(abrufbar unter: https://www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen-und-handlungshilfen/telefax-ist-nicht-datenschutz-konform-16111)

Deutsch E., Spickhoff A. (2014): XVII. Patientendaten: Dokumentation, Datenschutz, Einsicht und Herausgabe von Unterlagen, Schweigepflicht, Zeugnisverweigerungsrecht. In: Medizinrecht. Springer, Berlin, Heidelberg

Schmola, G. Hrsg, Rapp B. Hrsg. (2016): Datenschutz und IT-Sicherheit. In: Compliance, Governance und Risikomanagement im Krankenhaus

Info-Broschüre: Der Bayerische Landesbeauftragte für den Datenschutz informiert zum Thema Krankenhaus
(abrufbar unter: https://www.datenschutz-bayern.de/0/Broschuere_Krankenhaus.pdf)

Weichert, Thilo: Datenschutzrechte der Patienten
(abrufbar unter: https://www.datenschutzzentrum.de/artikel/779-Datenschutzrechte-der-Patienten.html#extended)

Datenschutz-Folgenabschätzung für die von der Gesellschaft für Telematik zugelassenen Komponenten der dezentralen Telematikinfrastruktur (TI) nach § 306 Absatz 2 Nummer 1 SGB V in Bundestagsdrucksache 19/27652

Dauber, Harald (2018): DS-GVO und BDSG für Ärzte, Zahnärzte und Heilberufe

Bundesärztekammer, Kassenärztliche Bundesvereinigung (2021): Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis

Höpken/Neumann (2015): Merkblatt Datenschutz im Krankenhaus

Bibliographische Informationen der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet unter *http://dnb.ddb.de* abrufbar.

Mitarbeiterinformation Datenschutz im Krankenhaus – Merkblatt für Beschäftigte

978-3-89577-928-2

Georg Karl Bittorf, Stefan Strüwe
1. Auflage 2024

Autoren: Georg Karl Bittorf, Stefan Strüwe
Illustration: Evelyn Klaiber, Köln
Gestaltung und Satz: Matthias Lück, CreaTechs, Boppard
Bildnachweis (Cover): ASDF, Adobe Stock

Printed in Germany

Für dieses Merkblatt werden Staffelpreise angeboten.
Informationen unter: 02234/98949-26

Hinweis: Aus Gründen der Lesbarkeit wird auf die Aneinanderreihung von männlichen und weiblichen Personenbezeichnungen verzichtet und stattdessen jeweils nur eine Form verwendet. Selbstverständlich richten sich alle Ausführungen gleichermaßen an alle Beschäftigten.

Krankenhaus-IT JOURNAL
Fakten und Perspektiven der IT im Gesundheitswesen

DATAKONTEXT