Datenschutzrichtlinie

der

Ev. Krankenhaus
BETHESDA
zu Duisburg GmbH

Inhaltsverzeichnis

1. Einleitung

Im Krankenhaus werden sehr sensible Daten über Patienten, ihre Krankheiten und ihr soziales Umfeld bekannt. Diese Daten werden als besonderes Berufsgeheimnis, teilweise auch „Arztgeheimnis“ oder „Patientengeheimnis“ genannt, durch § 203 StGB besonders geschützt. Der Patient verlässt sich auf dieses absolute Vertrauen in die Verschwiegenheitspflicht des Arztes und des Personals.

Alle anderen Beschäftigten in einem Krankenhaus, wie auch Zivildienstleistende und technische Hilfskräfte, sind ebenso ständig mit sensiblen Daten konfrontiert und haben deshalb die ihnen zur Verfügung stehenden Daten ebenso vertraulich zu behandeln.

Selbst die Tatsache der Aufnahme in ein Krankenhaus ist bereits eine schutzwürdige Information. Dabei sind nicht nur Name und Anschrift schutzwürdig, sondern alle Möglichkeiten der Identifizierung, insbesondere bei Personen mit hohem Bekanntheitsgrad.

Als Grundprinzip des Datenschutzes und des Rechtes auf informationelle Selbstbestimmung gilt die Transparenz der Datenverarbeitung für den Betroffenen. Jeder Patient muss wissen, welche Daten zu welchem Zweck über ihn gespeichert und an wen diese weitergegeben werden. Nur so kann er seinen Anspruch auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch gegenüber dem Krankenhaus geltend machen.

Neben dem Schutz von schriftlichen Unterlagen (Verschluss) und unberechtigtem Zugang auf Datenverarbeitungssysteme (Passwortschutz) sollten auch geeignete Möglichkeiten gefunden werden, dass im Gespräch mit Patienten die Vertraulichkeit gewahrt wird und zufällig anwesende Mitpatienten oder Besucher keine Kenntnis von Befunden oder ärztlichen und pflegerischen Maßnahmen erhalten.

Im medizinischen Bereich sind die Offenbarungsmöglichkeiten gegenüber Dritten für den Arzt z.B. aufgrund der Vorschriften des Strafgesetzbuches stark eingeschränkt. Von seiner Schweigepflicht kann der Arzt nur vom Betroffenen selbst oder (in stark eingeschränktem Umfang) durch Gesetze befreit werden.

Da der Arzt für seine Leistung einschließlich der dazu notwendigen Dokumentation die Verantwortung übernimmt, dürfen z.B. auch Mitarbeiter und Gehilfen des Arztes, Pflegepersonal, medizintechnische Mitarbeiter und Hilfskräfte nicht diese Schwelle überschreiten.

Im Verwaltungsbereich bedarf die Datenerhebung und Datenspeicherung eines Vertrages und die Datenübermittlung an Dritte (z.B. Krankenkassen) einer Rechtsvorschrift. Auch hier sind nur Informationen an den Betroffenen selbst oder an Dritte nur durch berechtigte Mitarbeiter des Krankenhauses zulässig. Ärztliche Daten, die dem Verwaltungspersonal zur Erfüllung ihrer Aufgaben bekannt werden, unterliegen wiederum der Schweigepflicht nach dem Strafgesetzbuch.

Alle Mitarbeiter und für das Krankenhaus Beschäftigte sollten sich stets bewusst sein, dass Verstöße gegen die einschlägigen Schweigepflichten die Persönlichkeitsrechte Betroffener gefährden und mit Geld- oder Freiheitsstrafen geahndet werden können.

Die vom Klinikum zur Verfügung gestellte EDV-Infrastruktur darf von den Mitarbeitern ausschließlich zur Erfüllung ihrer dienstlichen Aufgaben genutzt werden. Jegliche private Nutzung ist zu unterlassen. Wir weisen hiermit ausdrücklich darauf hin, dass die EDV-Infrastruktur des Klinikums nicht dem Telekommunikationsgesetz (TKG) unterliegt und es keinen Schutz von persönlichen Daten gibt.

Diese Datenschutzrichtlinie ist eine Zusammenfassung.
Weitere Informationen finden Sie in dem Dokument „Erläuterung zur Datenschutzrichtlinie“.

2. Geltungsbereich

Die vorliegende Richtlinie regelt den Einsatz von Informationstechnologien in sämtlichen Bereichen der Evangelisches Krankenhaus BETHESDA zu Duisburg GmbH (kurz: EKB).

Sie regelt deren Nutzung im Hinblick auf die betrieblichen Anforderungen an die Datensicherung und die geltenden gesetzlichen Bestimmungen des Datenschutzes nach den Anordnungen des Bundesdatenschutzgesetzes (BDSG) und

weiteren datenschutzrechtlichen Gesetzen – insbesondere des Datenschutzgesetzes der Ev. Kirch Deutschland (DSG-EKD) – und Verordnungen.

3. Begriffsbestimmungen

a) ***Personenbezogene Daten*** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (betroffene Person).

b) ***Datenverarbeitung*** ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten.

c) ***Erheben*** (Erhebung) das Beschaffen von Daten über die betroffene Person,

d) ***Speichern*** (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,

e) ***Verändern*** (Veränderung) das inhaltliche Umgestalten gespeicherter Daten,

f) ***Übermitteln*** (Übermittlung) die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die verantwortliche Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden oder dass der Dritte zum Abruf in einem automatisierten Verfahren bereitgehaltene Daten abruft,

g) ***Sperren*** (Sperrung) das Verhindern weiterer Verarbeitung gespeicherter Daten,

h) ***Löschen*** (Löschung) das Unkenntlichmachen gespeicherter Daten,

i) ***Nutzen*** (Nutzung) jede sonstige Verwendung personenbezogener Daten, ungeachtet der dabei angewendeten Verfahren.

j) ***Verantwortliche Stelle*** ist die Stelle im Sinne des § 2 Abs. 8 DSG-EKD, die personenbezogene Daten in eigener Verantwortung selbst verarbeitet oder in ihrem Auftrag von einer anderen Stelle verarbeiten lässt.

k) ***Empfänger*** ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht die betroffene Person sowie diejenigen Personen oder Stellen, die im Inland oder im Übrigen Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union personenbezogene Daten im Auftrag verarbeiten.

l) ***Automatisiert*** ist eine Datenverarbeitung, wenn sie durch Einsatz eines gesteuerten technischen Verfahrens selbsttätig abläuft.

m) Eine ***Akte*** ist jede der Aufgabenerfüllung dienende Unterlage, die nicht Teil der automatisierten Datenverarbeitung ist.

n) ***Anonymisieren*** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

o) ***Pseudonymisieren*** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion Datenschutzgesetz Nordrhein-Westfalen – DSG NW Seite 9 nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Die datenverarbeitende Stelle darf keinen Zugriff auf die Zuordnungsfunktion haben; diese ist an dritter Stelle zu verwahren.

4. Organisation

Im Intranet befinden sich eine Datenschutzrichtlinie und eine Erklärung zum Datenschutz für jeden Mitarbeiter im Zugriff. Für das Krankenhaus gibt es einen durch die Geschäftsführung ernannten Datenschutzbeauftragten. Zusätzlich können in bestimmten Abteilungen oder Bereichen Personen benannt werden, die beratend und unterstützend für den Datenschutzbeauftragten tätig sind. Sie unterliegen der gleichen Schweigepflicht wie der Datenschutzbeauftragte.

5. Datenschutzbeauftragter

Datenschutzbeauftragter im EKB ist:

Herr Sascha Krause
Tel.: 2084 Email: s.krause@bethesda.de

6. Verpflichtungserklärung

a) Gemäß § 6 DSG-EKD ist es den bei der Datenverarbeitung tätigen Personen untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

7. Berechtigungskonzept

a) Der zuständige Abteilungsleiter hat ca. 4 Wochen vor Stellenantritt des neuen Mitarbeiters mit dem Formblatt „Anmeldeformular für Benutzeraccounts“ der ADV-Abteilung die benötigten Berechtigungen des neuen Mitarbeiters anzuzeigen.

b) Die ADV-Abteilung vergibt in Abhängigkeit von der Nutzung und der Beantragung des Abteilungsleiters bestimmte Zugriffsrechte für die jeweiligen Mitarbeitergruppen.

8. Hardware

a) Es ist nur die von der Dienststelle zur Verfügung gestellte Hardware zugelassen.

b) Privat beschaffte Hardware (auch Datenträger) darf ohne schriftliche Zustimmung der Geschäftsführung im Klinikum nicht benutzt werden. Für eine Einsatz < 24 Stunden z.B. Vorführung, Demonstrationen etc. ist eine rechtzeitige Absprache mit der ADV-Abteilung ausreichend.

c) Wurde einer dienstlichen Nutzung von privater Hardware durch die Geschäftsführung zugestimmt, muss die ADV-Abteilung zum Ende der Nutzung die Hardware prüfen und sicherstellen, dass alle klinikinternen Daten und Patientendaten gelöscht sind. Der Eigentümer hat das Ende der Nutzung rechzeitig der ADV anzuzeigen.

d) Die Installation neuer Hardware und die Anbindung an das Netzwerk erfolgt durch die ADV-Abteilung.

e) An der bereitgestellten Hardware dürfen keinerlei Veränderungen vorgenommen werden.

f) Sowohl die von der Dienststelle zur Verfügung gestellte Hardware, als auch die Nutzung von privater Hardware ist nur im Rahmen einer dienstlichen Tätigkeiten gestattet. Eine private Nutzung ist grundsätzlich nicht zulässig.

9. Software

a) Als Netzwerksoftware und Anwendersoftware, die allen Benutzern oder Benutzergruppen zur Verfügung steht (Windows, Excel usw.) darf nur die offiziell durch die Dienststelle freigegebene Software vorhanden sein.

b) Bei Anwendersoftware, die nur von bestimmten Dienststellen, Benutzergruppen oder auf Stand-Alone-Systemen genutzt wird, gilt Abs. a) entsprechend.

c) Dienstlich eigenentwickelte Software ist nach Überprüfung durch die ADV-Abteilung und bei Verarbeitung von vertrauenswürdigen Daten durch den Datenschutzbeauftragten zulässig.

d) Das Einspielen von privater Software und Dateien auch für dienstliche Zwecke ist nicht zugelassen. Dienstliche Software darf für private Zwecke nicht genutzt werden.

e) Ebenfalls nicht zugelassen sind Spielprogramme; dies gilt auch für die von Lieferanten dienstlicher Hard- und Software kostenlos angebotenen Spielprogramme.

f) Datenträger dürfen erst nach Überprüfung auf Virenbefall eingespielt werden. Verfahren (Programme, Software) und Daten dürfen nicht verfälscht und unbefugt an Dritte weitergeben werden.

10. Virenschutz

a) Bei allen PCs im EKB, welche mit einem lokalen Laufwerk ausgestattet sind, ist die Festplatte regelmäßig mit einem Viren-Scanner zu prüfen.

b) Alle fremden Datenträger (Disketten, Bänder etc.) sind vor der Verwendung mit einem Viren-Scanner zu prüfen. Falls vorhanden, ist hierzu ein separater PC zu verwenden, der nicht in das Datennetz vom EKB integriert ist.

c) Anlagen zu Emails sind zunächst auf Festplatte zu speichern und vor dem Öffnen mit einem Viren-Scanner zu prüfen.

d) Dateien und Programme, die über Internet oder von anderen Servern bezogen werden, sind vor dem lokalen Einsatz mit einem Viren-Scanner zu prüfen.

e) Werden tragbare Rechner (Laptops etc.) sowohl im geschützten Intranet der Verwaltung als auch im ungeschützten Internet benutzt (z.B. auf Dienstreisen), so ist in besonderem Maße dafür Sorge zu tragen, dass keine Computerviren oder Programme, die zum ausspähen von Daten verwendet werden können, über den tragbaren Rechner in das geschützte Verwaltungsnetz gelangen können. Dies erfordert, dass tragbare PCs vor jeder Verbindung mit dem Verwaltungsnetz auf Computerviren überprüft werden müssen.

f) Wenn der Verdacht auf Virenbefall besteht, ist grundsätzlich die verantwortliche ADV-Abteilung einzuschalten. Die Mitarbeiter der ADV-Abteilung bestimmen die zu ergreifenden Maßnahmen.

11. Umgang mit Datenträgern

a) Datenträger mit personenbezogenen Daten dürfen nicht an Unbefugte weitergegeben werden. Sie sind unter Verschluss zu halten.

b) Die Versendung von Datenträgern mit personenbezogenen Daten (z.B. Disketten) ist in einem verschlossenen Umschlag durchzuführen. Die Versendung bzw. die Übergabe ist schriftlich festzuhalten. Die Übergabe von Hand zu Hand ist vorzuziehen.

c) Da gelöschte Daten häufig mit speziellen Programmen wieder hergestellt werden können, dürfen elektronische Datenträger (z.B. USB-Stick) nach einmaliger Verwendung mit Daten aus dem Klinikum nicht mehr anders (Privat) verwendet werden. Ein Zugriff durch Dritte auf diese Datenträger darf nicht stattfinden. Eine andere Nutzung des elektronischen Datenträgers ist erst nach Löschung oder Formatierung des elektronischen Datenträgers und Freigabe durch die ADV-Abteilung gestattet.

12. Umgang mit Krankenakten

a) Der Umgang mit den Krankenakten obliegt allein dem ärztlichen Personal. Das Pflegepersonal, das Personal des Archivs, der Sozialdienst, der medizinische Schreibdienst und die Chefarztsekretärinnen handeln nur im Auftrag des Chefarztes, wenn sie Umgang mit der Krankenakte pflegen. Dieser Auftrag ist vom Chefarzt an die Personen die solche Funktionen ausführen grundsätzlich gegeben. Der Chefarzt hat jederzeit das Recht, ungeeignete Personen vom Zugriff auf die Krankenakten auszuschließen.

b) Der materielle Teil der Krankenakte ist Eigentum des Krankenhauses. Der schriftliche Inhalt gehört ausschließlich zum Verantwortungsbereich des jeweiligen Chefarztes. Die Akte darf aus Gründen des Beschlagnahmeverbotes das Krankenhaus nicht verlassen.

c) Der Krankenhausträger ist dafür verantwortlich, dass die Behandlungsunterlagen jederzeit verfügbar sind bzw. Klarheit über den Verbleib der Unterlagen besteht (z.B. zur Beweißerleichterung).

d) Der Chefarzt ist verantwortlich für die Sicherung und Wahrung des Patientengeheimnisses.

e) Die Erstellung, Bearbeitung und Verwendung der Krankenakte gehört in die Zuständigkeit der verantwortlichen Ärzte, soweit dies durch Verfahrensanweisungen oder Dienstanweisungen im Klinikum nicht anders geregelt ist.

f) Für die Archivierung und Vernichtung der Krankenakten ist die Krankenhausverwaltung verantwortlich.

g) Im Gefahrenfall (Brand, Evakuierung usw.) haben alle Mitarbeiter des Krankenhauses zum Zweck der Sicherstellung ein befristetes Zugriffsrecht. Der Inhalt der Krankenakte bleibt dabei unberührt.

h) Die Krankenakten sind vor unerlaubtem Zugriff durch Dritte zu sichern.

13. Datensicherung

a) Für die Sicherung der Daten ist die Krankenhausleitung / ADV-Abteilung verantwortlich (Ausgenommen sind Laptops und Stand-alone-Systeme).

b) Die Sicherungsmedien sind getrennt vom Speicherort (anderer Brandabschnitt oder anderes Gebäude oder brandsicherer Safe) aufzubewahren.

14. Datenspeicherung

a) Allgemein gilt, dass auf lokalen Datenträgern – also insbesondere auf der Festplatte – des PC‘s nur Programmdateien gespeichert werden dürfen, die sich im Fehlerfall mit überschaubarem Aufwand wiederherstellen lassen. Die mit diesen Programmen erzeugten Daten sollten in der Regel in bestimmten Verzeichnissen auf dem Server gespeichert werden.

b) Personenbezogene Daten dürfen auf lokalen Laufwerken (C:) und Datenträgern (A:) außer zur temporären Bearbeitung nicht gespeichert werden.

c) Das Abspeichern von personenbezogenen Daten oder anderen als vertraulich eingestuften Daten auf tragbaren Computern (Notebooks, Laptops,...) ist generell nicht gestattet, sofern die tragbaren Computer keine technischen Vorrichtungen haben, die einen Zugriff durch Dritte automatisch verhindern (zeitabhängige automatische Verriegelung, Verschlüsselung aller personenbezogenen Daten). Die Vorrichtung und die ausreichende Wirksamkeit zum Schutz der personenbezogenen Daten muss vor der Nutzung von der ADV-Abteilung geprüft und bestätigt werden.

d) Daten auf einem Netzwerklaufwerk werden täglich automatisch gesichert. Beim Ausfall der Festplatte im PC sind dagegen die Daten ein für alle Mal verloren! Jeder Anwender ist für die Sicherung seiner Daten auf lokalen Laufwerken selbst verantwortlich.

15. Datenvernichtung

a) Personenbezogene Daten in Papierform müssen mittels Papiershredder vernichtet oder in dafür speziell zu Verfügung gestellten Behältern entsorgt werden. Es dürfen keine lesbaren personenbezogenen Daten in den Hausmüll gelangen.

b) Datenträger, auf denen sich personenbezogene Daten befinden werden durch die ADV-Abteilung vernichtet. Disketten, CDs/DVDs oder andere Datenträger mit sensiblen Daten müssen vor der Verschrottung mechanisch zerstört werden.

16. Aktenlagerung / Archivierung

a) Krankenakten sind nach Abschluss der Behandlung 30 Jahre lang sicher aufzubewahren. Die hierfür nötigen Archivräume sind seitens des Krankenhauses geschaffen.

b) Archiv-, und Lagerräume sind verschlossen zu halten und gegen nnbefugten Zugriff zu sichern.

c) Alle nicht zu archivierenden Unterlagen der Krankenakte und alle nicht in die Krankenakte eingefügten Patientenunterlagen (dies können sein: Aufzeichnungen, Untersuchungsergebnisse sowie deren Kopien usw.) sind datenschutzrechtlich zu vernichten. Das heißt, diese Unterlagen sind mittels eines Aktenvernichters mit einer maximalen Streifenbreite von 4 mm nach DIN 32757 zu entsorgen.

17. Magnetbandkassetten / Diktierdateien

a) Datenträger aus Diktiergeräten verbleiben grundsätzlich in den Räumen des Krankenhauses.

b) Datenträger sind vor dem ersten Gebrauch mit einer laufenden Nummer sowie mit den Namen des Arztes zu versehen.

c) Der Diktierende hat seinen Namen, das Datum des Diktates und die Datenträgernummer in der Krankenakte zu vermerken.

d) Nach erfolgter Übertragung ist der Datenträger nach Rücksprache mit dem Inhaber von der/dem zuständigen Mitarbeiter(in) zu löschen und an den Besitzer zurückzugeben.

e) Defekte Datenträger sind datenschutzrechtlich zu entsorgen.

f) Diensträume der Ärzte, Sekretariate und Büros sind beim Verlassen abzuschließen.

18. Verhalten im Netz von EKB

a) Das Intranet des EKB kann von jedem Mitarbeiter uneingeschränkt genutzt werden.

b) Auch wenn die Mitarbeiter des Krankenhauses ohne Berechtigungsprüfung auf viel Inhalte des Intranets Zugriff haben handelt es sich nicht um eine öffentliche Plattform. Alle Informationen aus dem Intranet des Krankenhauses unterliegen der betrieblichen Schweigepflicht und dürfen nicht ohne Zustimmung der Geschäftsführung anders verwendet oder an Dritte weitergegeben werden.

c) Ebenso wie im Internet sind alle bekannten Regeln der Rücksichtnahme, des Anstandes und Rechtes einzuhalten.

d) Im Intranet gibt es Bereiche die nur Mitarbeitern mit ausreichender Berechtigung zugänglich sind. Es ist darauf zu achten, sich beim Verlassen des Arbeitsplatzes abzumelden, um ungewollten Zugriff durch Dritte zu vermeiden.

19. Verhalten bei Arbeitsunterbrechung

a) Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

b) Räume oder Datenverarbeitungsanlagen, in/mit denen personenbezogene Daten verarbeitet werden, sind bei Abwesenheit der berechtigten Personen, auch wenn dies nur vorübergehend ist, zu verschließen/zu sichern. Gleichzeitig sollte ein Passwortschutz im Bios oder Vergleichbarem eingerichtet werden.

c) Datenträger mit personenbezogenen Daten (Disketten, Ausdrucke), sofern nicht mit ihnen gearbeitet wird, sind unter Verschluss zu halten.

20. Passwortregeln

a) Werden Softwaresysteme oder einzelne Dateien durch die Eingabe eines persönlichen Geheimwortes – das so genannte Passwort – geschützt, ist dieses Passwort unbedingt geheim zu halten. Passwörter dürfen weder an Arbeitskollegen, an Vorgesetzte noch an andere Personen weitergegeben werden.

b) Das Passwort ist zu ändern, wenn der Verdacht besteht, dass es jemand anderes in Erfahrung gebracht hat.

c) Für den Vertretungsfall und bei Erfordernis des Datenzugriffes sind abteilungsinterne Regelungen festzulegen.

d) Passwörter sind mindestens 6 Stellen lang (möglichst 8 Stellen) und sollten aus Buchstaben und Ziffern bzw. Sonderzeichen bestehen.

e) Passwörter, welche Sie innerhalb des Krankenhauses benutzen, sollten nicht mit Passwörtern übereinstimmen, die privat, z. B. bei der Einwahl in Online-Dienste genutzt werden.

f) Beachten Sie, dass das Softwarezugangssystem so ausgerichtet wurde, dass der Zugang nach drei (oder fünf) Fehlversuchen der Passworteingabe gesperrt wird.

g) Passwörter dürfen nicht in Dateien gespeichert werden oder auf programmierbare Funktionstasten gelegt werden. Zettelpasswörter sind verboten.

21. Auskunft an Patienten

a) Per Gesetz ist dem Patienten auf Wunsch die Einsicht in seine Krankenakte unentgeltlich zu gewähren. Eine Einsichtnahme ist grundsätzlich vom verantwortlichen Chefarzt zu prüfen und zu veranlassen.

b) Eine Einsichtnahme in die Krankenakte steht dem betroffenen Patienten nicht zu, wenn berechtigte Geheimhaltungsinteressen Dritter, deren Daten zusammen mit denen des Patienten aufgezeichnet sind, überwiegen.

c) Die Einsichtnahme in die Krankenakte kann dem Patienten ebenso verweigert werden, wenn die Gefahr besteht, dass die enthaltenen Informationen ihm schaden können.

d) Der Patient kann gewünschte Kopien aus seiner Krankenakte (Patientenakte) erhalten. Dies ist vom Patienten schriftlich zu beantragen. Die Kosten hierfür werden dem Patienten in Rechnung gestellt.

e) Einen Anspruch auf Aushändigung der Originalunterlagen hat der Patient per Gesetz nicht. In allen anderen begründeten Ausnahmefällen einer Übergabe von Originalunterlagen hat der entsprechende Chefarzt das Verlangen zu prüfen und sich die Ausleihe durch die Geschäftsführung **schriftlich** genehmigen zu lassen. In diesem Fall verbleibt eine Kopie in der Krankenakte mit dem Vermerk des Verbleibes der Originalunterlagen.

22. Auskunft an Dritte

a) Bei Einsichtnahme durch Dritte, z.B. Angehörige des Patienten, beauftragte Rechtsanwälte usw., muss eine entsprechende Schweigepflichtentbindung des betroffenen Patienten vorliegen.

b) Im Todesfall bzw. bei Entmündigung eines Patienten muss der Verwandtschaftsgrad zum Patienten berücksichtigt werden bzw. die Vormundschaft belegt werden. Sofern nicht eindeutig belegbar, ist die Rechtmäßigkeit durch die Geschäftsführung zu prüfen.

c) Die Einsicht hat immer unter Anwesenheit des ärztlichen Personals zu erfolgen. In Ausnahmefällen können Sekretärinnen oder Pflegepersonal für die Anwesenheit bei der Einsichtnahme beauftragt werden.

23. Übermittlung an Krankenkassen

a) Krankenkassen dürfen Daten nur mit Befugnis erheben. Eine Verpflichtung des Krankenhauses gegenüber den Krankenkassen zur Übermittlung von Entlassungsberichten, Arztbriefen, Befundberichten, Gutachten, Röntgenaufnahmen, usw. besteht nicht.

b) Für EKB wird festgelegt, dass Unterlagen aus Krankenakten nur nach Anforderung durch den Medizinischen Dienst der Krankenkasse (MDK) direkt an diesen überstellt werden dürfen. Selbst das Versenden von medizinischen Unterlagen in einem verschlossenen Umschlag mit Patientenname und dem Hinweis „Nur für den MDK bestimmt“ an die Krankenkassen sind **unzulässig**.

c) Bei weiteren Anforderungen seitens der Krankenkassen werden diese mit einer Kopie des Grundsatzurteiles zurück gesendet. Sollte bei der Einholung von Unterlagen durch die Krankenkassen eine Einwilligungserklärung des Versicherten zur Übermittlung der Unterlagen beigefügt sein, so stellt dies eine Umgehung der gesetzlichen Regelung dar. Die Forderung der Krankenkassen an Krankenhäuser und Ärzte unter Vorlage der Einwilligungserklärung ist rechtlich nicht gedeckt und damit unzulässig. Es ist analog wie oben genannt zu verfahren.

d) Die vorgeschriebene Übermittlung von Daten an die Krankenkassen gemäß §301 SGB V, d.h. die medizinischen Begründungen für die Überschreitung der Dauer der Krankenhausbehandlung, bleiben von dieser Regelung unberührt.

24. Bildschirmarbeitsplätze

a) Die Einrichtung der Bildschirmarbeitsplätze muss in Anlehnung an die Bildschirmarbeitsplatzverordnung geschehen. Eine Veränderung des Arbeitsplatzes ist nur nach vorheriger Absprache mit dem Vorgesetzten und dem Sicherheitsbeauftragten zulässig.

25. Internet

a) Der Internet-Zugang darf ausschließlich für die Erfüllung geschäftlicher Aufgaben genutzt werden.

b) Das Internet darf nur mit der gültigen persönlichen Zugangsberechtigung genutzt werden. User-ID und Passwort dürfen nicht an Dritte weitergegeben werden. User-ID und Passwort eines Dritten dürfen nicht verwendet werden.

c) Bei Informationen aus dem Internet ist darauf zu achten, dass nur bekannte bzw. nachprüfbare Informationsquellen genutzt werden.

d) Das Abrufen, Anbieten oder Verbreiten von rechtswidrigen Inhalten, insbesondere solchen, die gegen strafrechtliche, datenschutzrechtliche, persönlichkeitsrechtliche, lizenz- oder urheberrechtliche Bestimmungen verstoßen, ist unzulässig.

e) Das Abrufen, Anbieten oder Verbreiten von politischen, diskriminierenden, diffamierenden oder verfassungsfeindlichen Informationen (z. B. rassistischer, sexistischer, pornografischer Art) ist verboten.

f) Die ADV-Abteilung weist ausdrücklich darauf hin, dass die Einhaltung dieser Grundsätze durch Einsatz elektronischer Abfragen überprüft wird (Protokollierung).

g) Verstöße gegen diese Regeln können arbeitsrechtliche oder sonstige Konsequenzen zur Folge haben.

26. Email

a) Das Versenden von Emails ist nur im Rahmen der dienstlichen Tätigkeit erlaubt.

b) Der elektronische Briefkasten sollte regelmäßig (täglich) hinsichtlich des Eingangs elektronischer Post überprüft werden.

c) Offensichtlich unsinnige E-Mails von unbekannten Absendern sollten ungeöffnet gelöscht werden. Gleiches gilt für die Anhänge von Mails aus nicht zuverlässigen oder unbekannten Quellen.

d) E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern sind hinsichtlich des Inhalts zu überprüfen (zweifelhafter Text, fehlender Bezug zu konkreten Vorgängen etc.).

e) Bei mehreren E-Mails mit gleich lautendem Betreff ist Vorsicht geboten.

f) Nur vertrauenswürdige Dateianhänge (Attachments) dürfen geöffnet werden.

g) Kein Doppelklick bei ausführbaren Programmen (z. B. *.COM, *.EXE) oder Script-Sprachen (z. B. *.VBS, *.BAT) sowie Bildschirmschonern (*.SCR). Vorsicht auch bei Office-Dateien (*.DOC, *.XLS, *.PPT). Auch eine E-Mail im HTML-Format kann aktive Inhalte mit Schadensfunktion enthalten.

h) Die Weiterleitung von Nachrichten im Vertretungsfall oder eine automatische Antwort für den Absender ist zu gewährleisten (Abwesenheitsagent).

i) Personenbezogene und vertrauliche Nachrichten sind physikalisch zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist.

j) Elektronische Irrläufer sind nach Möglichkeit an den richtigen Adressaten weiterzuleiten. Ist dieser nicht zu ermitteln, muss die E-Mail an den Absender zurückgeschickt werden.

k) Sensible personenbezogene oder sonstige vertrauliche Informationen dürfen nur unter Einsatz geeigneter Verschlüsselungsverfahren elektronisch übertragen werden. Das Gleiche gilt für beigefügte Anlagen.

l) Der Versand von Kettenbriefen und Mails ist verboten.

m) Word-Dokumente sind möglichst im PDF-Format zu versenden, da hierzu keine Makrosprache existiert und damit keine Gefahr von Makroviren besteht.

n) Zur Vermeidung einer fehlerhaften Zustellung müssen E-Mails eindeutig adressiert werden.

o) Grundsätzlich darf keiner Aufforderung zur Weiterleitung von Mails oder Anhängen ohne strenge Prüfung gefolgt werden.

p) Gelegentlich ist zu prüfen, ob sich E-Mails im Postausgangskorb befinden, die nicht vom Benutzer selbst verfasst wurden.

q) Bei der Vergabe von Mailkennungen (Adressen) sollen Funktionsadressen / Abteilungsadressen verwendet werden. (z.B. sekretariat.orthopaedie@.... oder leitung.haustechnik@...)

r) In Ausnahmefällen ist die Vergabe von namentlichen Postfächern für einen reibungslosen Ablauf des Betriebes sinnvoller (Bekanntheitsgrad des Mitarbeiters, Leitungsfunktionen mit vertraulichen Informationen/Aufgaben). Auch wenn Mitarbeiter eine Mailkennung mit ihrem persönlichen Namen erhalten (z.B. m.mustermann@bethesda.de) handelt es sich nicht, um ein persönliches Postfach gem. Telekommunikationsgesetz (TKG). Es handelt sich weiterhin um ein Funktionspostfach. Der Mitarbeiter muss damit rechnen, dass bei Abwesenheit (Urlaub oder Krankheit) auf Anordnung des Vorgesetzten oder der Geschäftsführung Zugriff auf das Postfach genommen wird.

28. Telekommunikationsanlage

a) Dienstliche Telefongespräche sind Gespräche, die ausschließlich dienstlich veranlasst sind.

b) Als dienstliche Telefongespräche gelten auch Privatgespräche, die dienstlich veranlasst sind oder einen unmittelbaren Einfluss auf Dienstplanung und -ablauf haben. Dazu gehören Gespräche, die wegen notwendiger privater Terminänderungen aus dienstlichen Gründen, Festsetzung von Arztterminen und Terminen von Rehabilitationsmaßnahmen, Mitteilungen an die Familie aufgrund von Mehrarbeit, Überstunden und Schichtwechsel, Vorbereitung von persönlicher Aus- und Weiterbildung, soweit diese arbeitsvertraglich gefordert ist, und mit Behörden, Arbeitnehmerorganisationen und arbeitsrechtlichen Beiständen geführt werden. Sie unterliegen der Zielnummerndokumentation.

c) Private Telefongespräche sind mit Ausnahme von (b) nicht dienstlich veranlasst und werden mit einem Code eingeleitet, der diese als Privatgespräch kennzeichnet. Sie können grundsätzlich von jedem fernamtsberechtigten Apparat geführt werden.

d) Bei internen und von außerhalb eingehenden Gesprächen erfolgt keine Erfassung der Gesprächsdaten.

e) Die Daten aller auslaufenden Telefongespräche werden erfasst. Dabei werden die folgenden Gesprächsdaten von der TK-Anlage im Digitalspeicher der TK-Anlage und deren Gebührenrechner aufgezeichnet: Rufende Nummer / Zielnummer / Datum (Tag, Monat, Jahr) / Code der Gesprächsart (dienstlich/privat) / Gebühreneinheiten.

29. Telefaxversand

a) Die Installation von Telefaxgeräten (auch durch Sponsoring) bedarf der Zustimmung der Geschäftsleitung.

b) Die Geräte sind so aufzustellen, dass Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Telefax-Schreiben erhalten.

c) Grundsatz: Was am Telefon nicht gesagt werden darf, darf auch nicht gefaxt werden!

d) Vergewissern Sie sich, wenn Sie einem Partner längere Zeit kein Fax gesendet haben, ob dessen Anschlussnummer noch stimmt.

e) Prüfen Sie, ob die zurückgesandte Anschlusskennung mit der übereinstimmt, die Sie anwählen wollten. Brechen Sie ggf. die Übermittlung sofort ab!

30. Nutzung von mobilen Computern

a) Das Notebook sowie das mitgelieferte Zubehör sind Eigentum des EKB. Für die pflegliche Behandlung der Geräte und sichere Aufbewahrung außerhalb des Klinikums sind Sie verantwortlich.

b) Eine Nutzung des Notebooks ist nur im Rahmen der dienstlichen Aufgaben zugelassen.

c) An den Geräten dürfen keine technischen Veränderungen vorgenommen werden.

d) Bei Mitnahme im Auto ist das Notebook nach Verlassen des Fahrzeuges mitzuführen. Bei kurzzeitigen Stopps bzw. dienstlichen Absprachen ist das Notebook im Kofferraum zu deponieren.

e) Durch Anschluss an das Klinik-Netz sind regelmäßig die neu erfassten Daten in das Klinik-Netz zu überspielen (Datensicherung). Gleichzeitig wird das Virenschutzprogramm aktualisiert. Ein Anschluss des Notebooks an andere Netze (z.B. zuhause ins Internet) ist nicht gestattet.

f) Das Kopieren der Software der Einrichtungen oder das Installieren zusätzlicher privater Software ist untersagt. Installationswünsche sind mit dem Abteilungsleiter/ Bereichsleiter und der ADV-Abteilung zu klären.

g) Die Ihnen zugewiesenen Passwortmechanismen sind nur für Sie bestimmt. Eine Weitergabe von Passworten oder ihre „Veröffentlichung“, z. B. durch einen Aufkleber am Gerät, sind unzulässig. Zettelpasswörter sind ebenfalls untersagt.

h) Das Gerät darf keinem anderen Nutzer (Anwender) zur Verfügung gestellt werden. Bei der Nutzung ist darauf zu achten, dass eine Kenntnisnahme von Daten des Klinikums durch Dritte nicht möglich ist.

i) Alle Daten des Klinikums sind in einem verschlüsselten Ordner auf dem Notebook zu speichern. Hierdurch soll sichergestellt werden, dass bei Verlust oder Diebstahl ein Zugriff durch Dritte nicht möglich ist.

j) Eine Vervielfältigung jedweder Daten (z.B. Ausdrucke, elektronische Kopien) vom Notebook außerhalb des Klinikums ist ohne ausdrückliche, schriftliche Genehmigung durch die Geschäftsführung des Klinikums verboten und erfüllt den Tatbestand des Datendiebstahls. Sofern eine Genehmigung zur Erstellung von Ausdrucken oder elektronischen Kopien erteilt wurde, sind nicht (mehr) benötigte Ausdrucke ordnungsgemäß in der Dienststelle zu vernichten und nicht mehr benötigte elektronische Kopien (ggf. physikalisch) in der Dienststelle zu löschen. (Siehe auch Pkt. 11 Umgang mit Datenträgern)

31. Heimarbeit / Telearbeit

a) Sofern im Folgenden nicht anders beschrieben, gelten für den Betrieb und die Nutzung des Heim-/Telearbeitsplatzes alle Regelungen und Vorschriften eines Klinikarbeitsplatzes.

b) Sämtliche vom Krankenhaus zur Verfügung gestellten Geräte und Software sind Eigentum des Krankenhauses und müssen mit der gebotenen Sorgfalt behandelt werden. Das schließt den Schutz vor schädigenden Einwirkungen (wie Hitze, Nässe, Stäube, Stöße, Magnetfelder), vor unbefugter Nutzung beispielsweise durch Dritte (auch Familienangehörige) sowie Diebstahl ein.

c) Zur häuslichen Verarbeitung vorgesehene Daten werden nur in dem erforderlichen Umfang von einem besonders benannten Mitarbeiter der Dienststelle (des Unternehmens) auf Datenträger kopiert und nach Bearbeitung wieder in das dienstliche System eingestellt. Sofern das lokale System eine direkte Netzwerkverbindung (z.B. VPN-Tunnel) zum Klinikum hat, dürfen nur die Funktionen und die Daten genutzt werden, welche zur Erfüllung der dienstlichen Aufgaben notwendig sind.

d) Der Aufstellungsort des Heim-/Telearbeitsplatzes ist so zu wählen, dass während der Arbeit an dem Heim-/Telearbeitsplatz die Kenntnisnahme von Daten des Klinikums durch Dritte (auch Familienangehörige) nicht möglich ist.

e) Bei lokal installierten Systemen ist in angemessenen Zeitabständen nach schädlichen Programmen (mittels „Virenscanner“ usw.) zu suchen. Auf die korrekte Funktion (keine unklaren Meldungen) des Virenscanners ist zu achten. Im Zweifel, ist die ADV-Abteilung des Klinikums zu unterrichten, um die weiteren Schritte zu besprechen.

f) Eine Vervielfältigung jedweder Daten (z.B. Ausdrucke, elektronische Kopien) am Heim-/Telearbeitsplatz ist ohne ausdrückliche, schriftliche Genehmigung durch die Geschäftsführung des Klinikums verboten und erfüllt den Tatbestand des Datendiebstahls. Sofern eine Genehmigung zur Erstellung von Ausdrucken oder elektronischen Kopien erteilt wurde, sind nicht (mehr) benötigte Ausdrucke ordnungsgemäß in der Dienststelle zu vernichten und nicht mehr benötigte elektronische Kopien (ggf. physikalisch) in der Dienststelle zu löschen. (Siehe auch Pkt. 11 Umgang mit Datenträgern)

g) Reparaturen, Wartungen usw. dürfen nur durch die ADV-Abteilung oder von ihr beauftragten Personen/Firmen durchgeführt. Sofern die Reparatur/Wartung auch durch den Anwender durchführbar ist, muss dieses in Rücksprache mit der ADV-Abteilung geschehen.

32. Videoüberwachung

a) Auf dem Gelände und in den Gebäuden des EKB gelangt eine Videoanlage zum Einsatz. Diese dient der Information zur Steuerung der Schranken in den Einfahrbereichen und zur Überwachung von Gebäudezugängen und Verkehrswegen.

b) Die Beobachtung öffentlich zugänglicher Räume und Bereiche des EKB erfolgt zur Wahrnehmung des Hausrechtes.

c) Eine Überwachung von festen Arbeitsplätzen der Mitarbeiter ohne Zustimmung der MAV und der dort tätigen Mitarbeiter findet nicht statt.

d) Die an diesen Orten anwesenden Mitarbeiter können mit den Videoanlagen erfasst werden. Die mit der vorhandenen Videoanlage erhobenen Bilddaten werden nur kurzzeitig zwischengespeichert. Die Anlage ist damit keine Videoüberwachungseinrichtung im Sinne § 6 Bundesdatenschutzgesetz.

e) Die Videoaufzeichnungen (Bilddaten) werden nur ausgewertet, wenn Unregelmäßigkeiten festgestellt wurden, Geräte oder sonstige Einrichtungsgegenstände abhanden gekommen oder sonstige strafbaren Handlungen aufgetreten sind.

f) Die Auswertung der Videoaufzeichnungen ordnet der Geschäftsführer bzw. der Verwaltungsleiter sowie sein Stellvertreter im Benehmen mit der MAV an.

33. Patienteninformation zum Datenschutz

a) Dem Patienten ist bei Aufnahme das Merkblatt zum Datenschutz / Einverständniserklärung in der gültigen Fassung auszuhändigen und unterschreiben zu lassen.

b) Diese Einverständniserklärung wird in der Verwaltung mit den Patientendaten hinterlegt.

34. Ausscheiden von Mitarbeitern

a) Vor dem Ausscheiden bzw. der Versetzung ist nach Möglichkeit eine Einweisung des Nachfolgers durchzuführen.

b) Von dem Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern.

c) Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen.

d) Ist die ausscheidende Person ein Funktionsträger in einem Notfall, so ist der Notfallplan zu aktualisieren.

e) Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere die ADV-Abteilung, sind vom Leiter der Fachabteilung über das Ausscheiden des Mitarbeiters zu unterrichten.

f) Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt, insbesondere zu Räumen mit IT-Systemen zu verwehren.

g) Sind Daten des Mitarbeiters in elektronischen Verzeichnissen des EKB veröffentlicht, sind diese zu löschen. Unbeschadet dessen gelten die gesetzlichen Löschfristen.