UNIVERSITÄT LEIPZIG
Medizinische Fakultät

Universitätsklinikum Leipzig
Medizin ist unsere Berufung.

Vertraulichkeitserklärung
zur Beachtung des Datenschutzes, insbesondere zur Wahrung der Vertraulichkeit, und zur Wahrung des Geschäfts- und Betriebsgeheimnisses

☐ **Anlage zum Vertrag:** _____

☐ **Einmaliger Auftrag am:** _____

Firma / Organisation
Adresse _____

Name, Vorname, Geburtsdatum des Vertretungsberechtigten bzw. des Einzelverpflichteten (Vertragspartei) _____

Hiermit bestätigt die Vertragspartei, dass sie selbst oder alle Mitarbeiter und sonstigen von ihm beauftragten Personen zur Einhaltung der nachfolgenden Regelungen verpflichtet sind.

Nach **Art. 5 DS-GVO sowie gem. § 203 StGB i.V.m. § 1 VerpflG in der jeweils geltenden Fassung** wird die Vertragspartei wie folgt auf die Wahrung der Vertraulichkeit sowie die sonstigen bei seiner Tätigkeit zu beachtenden Vorschriften über den Datenschutz, wie beispielsweise das Sächsische Krankenhausgesetz (SächsKHG) und das Sächsische Datenschutzdurchführungsgesetz (SächsDSDG) und das Geschäfts-, Betriebsgeheimnis sowie den Umgang mit Software verpflichtet:

Aufgrund Ihrer arbeitsvertraglichen bzw. sonstigen vertraglichen Bindung zur zeitweiligen Aufgabenerfüllung (bspw. als Dienstleister, oder Gastarzt, Hospitant, Praktikant, Schüler u. ä.) am/für das Universitätsklinikum Leipzig AöR (UKL), der Medizinischen Fakultät der Universität Leipzig (MF) bzw. der Medizinischen Berufsfachschule (MBFS) sind Sie zur Wahrung

1. **des Geschäfts- und Betriebsgeheimnisses**
2. **der Vertraulichkeit beim Umgang mit personenbezogenen Daten (Datenschutz)**
3. **dem ordnungsgemäßen Umgang mit Software**

verpflichtet.

1. Geschäfts- oder Betriebsgeheimnis

Die Vertragspartei ist zur Geheimhaltung aller Informationen verpflichtet, die ihr im Zusammenhang mit der übernommenen Aufgabe bekannt werden und die nicht offenkundig sind. Dies gilt sowohl für Informationen über das UKL, die MF und die MBFS sowie auch über deren Geschäftspartner. Diese Geheimhaltungsvorschrift besteht auch nach Beendigung Ihrer Tätigkeit fort.

2. Vertraulichkeit beim Umgang mit personenbezogenen Daten (Datenschutz)

Es ist der Vertragspartei untersagt, personenbezogene Daten ohne entsprechende Befugnis, die sich nach Art. 6 und Art. 9 DS-GVO, §§ 33 Abs. 2, 34 SächsKHG sowie §§ 3, 4 SächsDSDG nur aus einer Rechtsvorschrift (u. a. Gesetz, Rechtsverordnung, Satzung) oder der Einwilligung des Betroffenen ergeben kann, zu verarbeiten.

"Verarbeitung" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Dies ist unabhängig davon, ob diese Daten in Erfüllung Ihrer Dienstaufgaben oder rein zufällig zu Ihrer Kenntnis gelangt sind.

"Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; in Dateiform oder als Akte (z.B. Aufzeichnungen auf maschinell lesbaren Datenträgern, Angaben auf Formularen und Karteikarten, allg. Arbeitsunterlagen, Röntgenbilder, Ultraschall-Aufnahmen, CT/MRT-Schnittbilder, Mikrofilme, Bild- und Tonträger u. a.) Unter personenbezogenen Daten sind nicht nur Daten von Mitarbeitern zu verstehen, sondern vor allem auch Patientendaten, einschließlich von deren Angehörigen, anderer Bezugspersonen oder sonstiger Dritter. Gesundheitsdaten unterliegen als Kategorie besonderer personenbezogener Daten einem ausgesprochen hohen Schutz.

Eine Verletzung der standesrechtlichen **"Ärztlichen Schweigepflicht"** (Muster-Berufsordnung für Ärzte, Apotheker) ist nach Strafgesetzbuch auch für die **„berufsmäßig tätigen Gehilfen“** unter Strafe gestellt, d.h. auch für Gesundheits- und Krankenpfleger/-innen, Hebammen/Entbindungspfleger, Med.-technische Assistenten/Assistentinnen, Diätassistenten/-assistentinnen, Arzthelfer/-innen, Praktikanten/Praktikantinnen, Verwaltungspersonal usw.

3. Ordnungsgemäßer Umgang mit Software

Der nicht ordnungsgemäße Erwerb, die Nutzung und das Inverkehrbringen von Computer-Software stellen Verstöße gegen das Urheberrecht, Strafrecht sowie einschlägige andere Rechtsnormen dar und kann sowohl gegenüber dem UKL / der MF als auch gegenüber

der Vertragspartei straf- und zivilrechtlich geahndet werden. Weiterhin besteht eine Gefahr hinsichtlich des Einsatzes von schadenstiftender Software (illegale Software-Kopien, Viren u. a.).

Deshalb ist festgelegt:

a) Software muss grundsätzlich ordnungsgemäß erworben und installiert werden (auch Demonstrations- und Test-Software). Der Erwerb erfolgt über den Bereich 1 – Informationssysteme des UKL, ebenso die Installation bzw. diese in Absprache. Analog für die Software-Deinstallation und die Verschrottung von Computern, inkl. der zuverlässigen Löschung von Daten.
b) Die Benutzung von Software, die nicht der direkten Aufgabenerfüllung dient, ist grundsätzlich untersagt.
c) Installierte Viren-Scanner dürfen nicht abgeschaltet bzw. deinstalliert werden.

Rechtsfolgen

1. Verstöße gegen das Geschäfts- oder Betriebsgeheimnis können auf der Grundlage des Gesetzes zum Schutz von Geschäftsgeheimnissen und anderer Rechtsgrundlagen zivilrechtlich sowie strafrechtlich geahndet werden.
2. Aus der Verletzung der Vertraulichkeit ergeben sich arbeits-, straf- oder ordnungswidrigkeitsrechtliche Konsequenzen (gem. § 22 SächsDSDG Geldbuße bis zu 25 T€, als Straftat bis zu 2 Jahren Freiheitsstrafe). Der Versuch ist strafbar.
3. Die Verbreitung / Benutzung illegal kopierter Software kann nach dem Urheberrechtsgesetz geahndet werden.
4. Die Verbreitung / Benutzung von schadensstiftender Software kann strafrechtlich verfolgt werden.
5. Verstöße lösen auch zivilrechtliche Schadenersatzansprüche aus.

Ein Merkblatt mit Erläuterungen und den relevanten Rechtsvorschriften sowie eine Kopie der Verpflichtungserklärung werden ausgehändigt. Weitere Informationen mit datenschutzrelevanten Regelungen ergeben sich aus den Dienstvereinbarungen und Dienstanweisungen sowie weiteren innerbetrieblichen Regelungen.

Verpflichtung nach § 203 StGB

Des Weiteren erklärt die Vertragspartei, die Anforderungen des § 203 StGB und die strafrechtlichen Folgen einer Verletzung zu kennen.

Soweit die Vertragspartei hierzu nicht gesetzlich bereits verpflichtet ist, erklärt sie Folgendes:

1. Ich verpflichte mich zur gewissenhaften Einhaltung und Erfüllung der gesetzlichen Anforderungen. Insbesondere ist mir bekannt, dass meine Verschwiegenheit auch nach Beendigung des Vertragsverhältnisses, gleich welcher Art dieses ist, uneingeschränkt und zeitlich unbefristet fortbesteht.
2. Ich verpflichte mich darüber hinaus alle meine Mitarbeiter (Bestandsmitarbeiter und zukünftige neue Mitarbeiter), die im Rahmen des gegenständlichen Auftrages bzw. Vertragsverhältnisses mit den der besonderen Verschwiegenheitspflicht unterliegenden Daten in Berührung kommen, ebenso wirksam nach § 203 StGB zu verpflichten.
3. Ich sichere zu, soweit in Erfüllung des Auftrages durch mich / unser Unternehmen Dritte (Subunternehmer) oder Geschäftspartner (im Rahmen eines mehrstufigen Vertragsverhältnisses) zum Einsatz kommen, für eine gleiche Verpflichtung Sorge zu tragen. Über die strafrechtlichen Konsequenzen einer fehlerhaften oder mangelnden Verpflichtung bin ich informiert.

In allen Zweifelsfragen werde ich entsprechenden Rechtsrat vor einer Offenbarung von Geheimnissen, welche § 203 StGB unterliegen einholen.

Ort, Datum	**Unterschrift, Firmenstempel**

Merkblatt zur Verpflichtung zur Vertraulichkeit

Dienstspezifische Datenschutzhinweise

Stand: Oktober 2019

1a. Inwieweit und welche Art von **Auskünften bei Nachfragen von außerhalb am Telefon** gegeben werden dürfen, bestimmt der jeweils behandelnde Arzt. Die Auskünfte sind unter Beachtung des Patientenwillens und unter Berücksichtigung der Einzelfallsituation zu erteilen **und immer restriktiv zu handhaben** (nach der Art des Anrufes, nur Terminauskunft, ob Notfall, ggf. nur allgemeine Auskunft, Verweis an den behandelnden Arzt oder an einen vom Patienten benannten Angehörigen, separate Einbestellung, usw.).

1b. Über die Identität des Anrufenden ist sich zu vergewissern, bspw. durch Erfragen von Geburts-datum, Anschrift oder letztem Aufenthalt im UKL und/oder Vergleich der auf dem Display gezeigten Telefonnummer mit der „Nächste Angehörige“ - Telefonnummer des Patienten im SAP.

1c. Anfragen von juristischen Personen (bspw. Vereine, Unternehmen, Arbeitgeber oder Behörden) sollen immer schriftlich (auch als Fax) an das UKL gerichtet werden. Sofern telefonische Anfragen erfolgen, sind diese darauf hinzuweisen.

1d. **Im Zweifelsfall ist keine Auskunft zu erteilen.**

1e. Sofern im SAP auf der Stations- oder Ambulanzübersicht für einen Patienten die „Pförtnersperre“ eingetragen ist, bedeutet dies ein striktes Auskunftsverbot gegenüber allen (auch telefonisch)nachfragenden Privatpersonen oder unbefugten juristischen Personen, sogar darüber, ob sich der Patient überhaupt im Klinikum aufhält.

2. Die **ärztliche Schweigepflicht** gilt grundsätzlich auch gegenüber nahen Angehörigen des Patienten.

3. **Sensible Patientengespräche** dürfen von anderen Patienten nicht mitgehört werden können, ggf. ist dafür z. B. ein separater Raum zu nutzen.

4. Patientenunterlagen dürfen niemals am Stationsstützpunkt unbeaufsichtigt liegen gelassen werden und dürfen, ebenso wie Bildschirme, von anderen Patienten und Besuchern nicht einsehbar sein.

5. Patienten und ggf. begleitende Dritte dürfen in Untersuchungs- oder Behandlungsräumen nicht unbeaufsichtigt sein.

6. Sofern keine Kontrolle gewährleistet ist, sind Türen bei Verlassen des Stützpunktes oder des Dienstzimmers zu verschließen.

7. **Rezepte und Arzt-Stempel** sind für Patienten nicht sichtbar zu lagern und nach Dienstende in einem Schrank sicher vor dem Zugriff Dritter einzuschließen (dies gilt immer -auch während der Dienstzeit- für **BTM-Rezepte und das BTM-Bestellbuch**).

8. Vom Postdienst entgegengenommene Patientenpost und Pakete sind zu quittieren und dem Patienten unmittelbar zu übergeben.

9. Zu entsorgende patienten- und personalbezogene Dokumente gehören IMMER in die abgeschlossene Daten-Mülltonne, welche in der Regel im AWT-Raum steht, **keinesfalls in die normalen Papierkörbe!** Zwischenzeitlich können solche Unterlagen in einer gekennzeichneten, für Patienten nicht einsehbaren und nicht zugänglichen Ablage gesammelt werden.

10. Spam-verdächtige E-Mails sind dem Bereich 1 – Informationsmanagement per E-Mail an *spamverdacht@medizin.uni-leipzig.de* zu melden – und zwar **nur als Anlage in dieser E-Mail- Meldung. Anhänge solcher verdächtigen E-Mails dürfen keinesfalls geöffnet werden!**

11. Logins für Windows und Anwendungssoftware (z. B. SAP) dürfen ausschließlich persönlich genutzt werden und sind geheim zu halten. Die Weitergabe personengebundener Passwörter ist untersagt (darunter fällt auch z. B. das Anbringen eines „Merkzettels“ am Bildschirm). Sobald kein unmittelbarer Programmzugriff mehr erforderlich ist, hat eine Systemabmeldung zu erfolgen („ausloggen“).

12. Für Windows und SAP erfolgt nach 6 Monaten automatisch ein erzwungener Passwortwechsel.[1]

13. Das ***Laufwerk W:*** besitzt für jede Klinik einen eigenen Ordner und dient zum Speichern klinikbezogener Daten, der Zugriff ist auf die jeweiligen Klinikmitarbeiter beschränkt. Als besondere Vorsichtsmaßnahme können (versehentlich) gelöschte oder geänderte Dateien innerhalb von 4 Wochen auf Antrag des jeweiligen Ordnerverantwortlichen durch den Bereich 1 wiederhergestellt werden

14. Das ***Laufwerk V:*** ist das persönlich-dienstliche Laufwerk eines jeden Mitarbeiters, auf welches **ausschließlich** dieser Zugriff hat. **LW V:** ist von jedem PC im Medizinnetz aus zugreifbar und wird zentral durch den Bereich 1 gesichert. Ggf. lokal auf dem PC gespeicherte Daten sollen deshalb regelmäßig nach **LW V:** gesichert oder gleich dort gespeichert werden.

15. Es dürfen nur solche Fälle/Patientendaten aufgerufen und bearbeitet werden, welche sich aus der aktuellen Arbeitsaufgabe ergeben, in der Regel also nur die Fälle aktueller oder noch zu bearbeitender Patienten (etwa zur Befund- oder Terminsuche bzw. Dokumentation). **Insbesondere ist es Ihnen gem. DS-GVO, SächsKHG, SächDSDG, § 85 SGB X, § 203 StGB (Verletzung von Privatgeheimnissen) sowie im Rahmen Ihres Arbeitsvertrags untersagt, aus nicht dienstlichen Gründen Fälle/Daten Dritter (z.B. von Arbeitskollegen, Verwandten oder Bekannten) aufzurufen, einzusehen oder weiterzugeben.**

16. Bildschirme, welche durch Patienten/Besucher eingesehen werden könnten, sind durch einen Bildschirmschoner zu schützen (mit automatischer Aktivierung nach 5 Minuten).

17. Häufig genutzte Faxnummern sind einzuspeichern, um die Gefahr eines Verwählens zu vermeiden. Bei wichtigen Faxen soll eine telefonische Ankündigung beim Empfänger bzw. Rückfrage erfolgen, ob das Fax angekommen ist. Sendeberichte können bei Erfordernis dem Dokument beigeheftet werden. Das Fax - Journal ist als genereller Nachweis am Fax einzustellen und 1 Jahr aufzuheben.

18. In Soziale Medien, wie Facebook oder Twitter, gehören keine UKL-internen Informationen oder diesbezügliche Problemdiskussionen.

19. Bild-, Video- oder Tonaufnahmen von Patienten bzw. deren Verletzungen mit privaten mobilen Endgeräten, wie etwa Smartphones, und deren Weitergabe sind strengstens untersagt!

20. Gesonderte Regelungen des UKL, wie Verfahrens- und Dienstanweisungen, sind zu beachten.

21. Stellen Sie selbst Datenschutzverletzungen fest, teilen Sie dies Ihrem Vorgesetzten und auch direkt dem Datenschutzbeauftragten mit. Solche Probleme könnten u. U. zu schwerwiegenden Folgen für das UKL führen. Das UKL hat eine **gesetzlich vorgeschriebene Benachrichtigungspflicht gegenüber Patienten und Meldepflicht gegenüber Aufsichtsbehörden**, sollten Informationen in falsche Hände gelangt sein.

Bei Rückfragen wenden Sie sich direkt an:

Universitätsklinikum Leipzig AöR, Stabsstelle Datenschutz

E-Mail: dsb@uniklinik-leipzig.de

[1] Die letzten fünf genutzten Passwörter dürfen sich nicht wiederholen, das jeweilige Anwendungssystem gibt Hinweise zu den Mindestanforderungen an das neue Passwort, eine Anleitung finden Sie außerdem im Intranet auf der Seite von Bereich 1 Hinweise zum Generieren und Merken von Passwörtern finden Sie unter

Merkblatt zur Verpflichtung zur Vertraulichkeit

„Mitarbeiterbezogener Datenschutz" auf der „Datenschutz"-Intranet-Seite.

Merkblatt zur Verpflichtung zur Vertraulichkeit

Dienstspezifische Datenschutzhinweise

Stand: Oktober 2019

Datenschutz-Grundverordnung DS-GVO

Art. 5 Rechenschaftspflichten

(1) Personenbezogene Daten müssen

a. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können ("Rechenschaftspflicht“).

Art. 32 Sicherheit der Verarbeitung

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Sächsisches Krankenhausgesetz SächsKHG

§ 33 Datenschutz

(1) Soweit in diesem Gesetz nichts anderes bestimmt ist, sind die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden. Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser. Patientendaten sind auch die personenbezogenen Daten von Angehörigen, anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.

(2) Patientendaten dürfen unbeschadet anderer Rechtsvorschriften verarbeitet werden, soweit

1. dies im Rahmen des Behandlungsverhältnisses auf vertraglicher Grundlage mit einem Angehörigen eines Gesundheitsberufs, der dem Berufsgeheimnis unterliegt, oder durch andere Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, erforderlich ist; die Verarbeitung von Daten zu diesen Zwecken richtet sich nach den für die genannten Personen geltenden Geheimhaltungspflichten, oder,
2. dies zur Ausbildung oder Fortbildung erforderlich ist und dieser Zweck nicht in vertretbarer Weise mit anonymisierten Daten erreichbar ist.

Beruht die Verarbeitung auf einer Einwilligung des Patienten, bedarf diese einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

(3) Eine Übermittlung von Patientendaten an Personen und Stellen außerhalb des Krankenhauses ist nur zulässig, soweit sie erforderlich ist

1. zur Erfüllung einer gesetzlich vorgeschriebenen Behandlungs- oder Mitteilungspflicht,
2.
   a. zur Entscheidungsfindung der Krankenkassen, ob und inwieweit Präventions-, Rehabilitations- oder andere komplementäre Maßnahmen angezeigt sind,
   b. zur Durchführung des Behandlungsvertrages einschließlich der Nachbehandlung, soweit der Patient nach Hinweis auf die beabsichtigte Übermittlung nicht etwas anderes bestimmt hat,
3. zur Abwehr von gegenwärtigen Gefahren für das Leben, die Gesundheit oder die persönliche Freiheit des Patienten oder eines Dritten, sofern diese Rechtsgüter das Geheimhaltungsinteresse des Patienten deutlich überwiegen,
4. zur Durchführung qualitätssichernder Maßnahmen in der Krankenversorgung, wenn das Interesse der Allgemeinheit an der Durchführung der beabsichtigten Maßnahme die schutzwürdigen Belange des Patienten erheblich überwiegt,
5. zur Durchführung eines mit der Behandlung zusammenhängenden gerichtlichen Verfahrens,
6. zur Feststellung der Leistungspflicht, Abrechnung und Überprüfung der Wirtschaftlichkeit durch die Sozialleistungsträger,
7. zur Unterrichtung der Angehörigen, soweit der Patient nicht seinen gegenteiligen Willen kundgetan, hat oder sonstige Anhaltspunkte bestehen, dass eine Übermittlung nicht angebracht ist.
8. oder sie in einer anderen Rechtsvorschrift geregelt ist.

In anderen Fällen ist eine Übermittlung von Daten nur mit Einwilligung des Patienten zulässig. Absatz 2 Satz 2 und 3 gilt entsprechend.

(4) Stellen oder Personen, denen nach dieser Vorschrift personenbezogene Daten befugt übermittelt worden sind, dürfen diese nur zu dem Zweck verwenden, der die Befugnis begründet. Im Übrigen haben sie diese Daten unbeschadet sonstiger Datenschutzbestimmungen in demselben Umfang geheim zu halten wie das Krankenhaus selbst.

(5) Dem Patienten ist auf Antrag kostenfrei Einsicht, insbesondere in seine Krankendaten zu gewährleisten. Soweit Auskunfts- und Einsichtsansprüche medizinische Daten des Patienten betreffen,

darf sie nur der behandelnde Arzt erfüllen. Die Auskunfts- und Einsichtsansprüche können im Interesse der Gesundheit des Patienten begrenzt werden; durch berechtigte Geheimhaltungsinteressen Dritter werden sie eingeschränkt.

(6) Nach Abschluss der Behandlung unterliegen personenbezogene Daten, die in automatisierten Verfahren gespeichert und direkt abrufbar sind, dem alleinigen Zugriff der jeweiligen Fachabteilung. Dies gilt nicht für diejenigen Daten, die für das Auffinden der sonstigen Patientendaten erforderlich sind. Die Eröffnung des Direktzugriffs auf den Gesamtdatenbestand für andere Stellen im Krankenhaus ist unter den Voraussetzungen des Absatzes 2 nur mit Zustimmung der Fachabteilung zulässig.

(7) Der Krankenhausträger hat einen Datenschutzbeauftragten zu benennen.

(8) Soweit sich das Krankenhaus bei der Verarbeitung von Patientendaten eines Auftragsverarbeiters bedient, ist insbesondere sicherzustellen, dass dieser die § 203 des Strafgesetzbuches entsprechende Schweigepflicht einhält.

§ 34 Datenschutz bei Forschungsvorhaben

(1) Ärzte dürfen Patientendaten, die innerhalb ihrer Fachabteilung oder bei Hochschulen innerhalb ihrer medizinischen Einrichtungen, in den Universitätsklinika oder in sonstigen medizinischen Einrichtungen gespeichert sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten. Satz 1 gilt entsprechend für sonstiges wissenschaftliches Personal dieser Einrichtungen, soweit es der Geheimhaltungspflicht des § 203 des Strafgesetzbuches unterliegt.

(2) Zu Zwecken der wissenschaftlichen Forschung ist die Übermittlung von Patientendaten an Dritte und die Verarbeitung durch sie zulässig, soweit der Patient eingewilligt hat. § 33 Abs. 2 Satz 2 und 3 gilt entsprechend.

(3) Der Einwilligung des Patienten bedarf es nicht, wenn der Zweck eines bestimmten Forschungsvorhabens nicht auf andere Weise erfüllt werden kann und

1. das berechtigte Interesse der Allgemeinheit an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Patienten erheblich überwiegt oder
2. es nicht zumutbar ist, die Einwilligung einzuholen und schutzwürdige Belange des Patienten nicht beeinträchtigt werden. Die übermittelnde Stelle hat den Empfänger, die Art der zu übermittelnden Daten, die betroffenen Patienten und das Forschungsvorhaben aufzuzeichnen.

(4) Sobald es der Forschungszweck erlaubt, sind die personenbezogenen Daten derart zu verändern, dass sie keine Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person mehr sind. Soweit dies nicht möglich ist, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern, sobald es der Forschungszweck erlaubt; die Merkmale sind zu löschen, sobald der Forschungszweck erreicht ist.

(5) Soweit die Bestimmungen dieses Gesetzes auf den Empfänger von Patientendaten keine Anwendung finden, dürfen sie nur übermittelt werden,

1. wenn sich der Empfänger verpflichtet,
   a. die Daten nur für das von ihm genannte Forschungsvorhaben zu verwenden,
   b. die Bestimmungen des Absatzes 4 einzuhalten und
   c. dem Sächsischen Datenschutzbeauftragten auf Verlangen Einsicht und Auskunft zu gewähren, und
2. wenn der Empfänger nachweist, dass bei ihm die technischen und organisatorischen Voraussetzungen vorliegen, um der Verpflichtung nach Nummer 1 Buchst. b zu entsprechen.

Sächsisches Datenschutzdurchführungsgesetz SächsDSDG
§ 22 Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten, die nicht offenkundig sind, verarbeitet oder die Übermittlung durch unrichtige Angaben erschleicht.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfundzwanzigtausend Euro geahndet werden.

(4) Wer eine der in Absatz 1 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

Urheberrechtsgesetz UrhG
§ 106 Unerlaubte Verwertung urheberrechtlich gesicherter Werke

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 3 MantelTVÄ UKL, Verschwiegenheit

(2) Ärzte haben über interne Angelegenheiten, insbesondere Angelegenheiten, deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus. Die Regelung betrifft auch Schriftstücke, Aufzeichnungen und bildliche Darstellungen.

§ 3 HTV UKL, Verschwiegenheit

(2) Die Beschäftigten haben über Angelegenheiten, deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus.

§ 3 TVöD Länder

(2) Die Beschäftigten haben über Angelegenheiten, deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus.

§ 3 TV-Ä

(2) Die Ärzte haben über Angelegenheiten, deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus. Bei Unterlagen, die ihrem Inhalt nach von der ärztlichen Schweigepflicht erfasst werden, darf der Arbeitgeber nur die Herausgabe an den ärztlichen Vorgesetzten verlangen.

Gesetz zum Schutz von Geschäftsgeheimnissen GeschGehG
§ 23 Verletzung von Geschäftsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,

1. entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt,
2. entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder
3. entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut

worden oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt.

(2) Ebenso wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach Absatz 1 Nummer 2 oder Nummer 3 erlangt hat.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz entgegen § 4 Absatz 2 Nummer 2 oder Nummer 3 ein Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt.

(4) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer

1. in den Fällen des Absatzes 1 oder des Absatzes 2 gewerbsmäßig handelt,
2. in den Fällen des Absatzes 1 Nummer 2 oder Nummer 3 oder des Absatzes 2 bei der Offenlegung weiß, dass das Geschäftsgeheimnis im Ausland genutzt werden soll, oder
3. in den Fällen des Absatzes 1 Nummer 2 oder des Absatzes 2 das Geschäftsgeheimnis im Ausland nutzt.

(5) Der Versuch ist strafbar.

(6) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geschäftsgeheimnisses beschränken.

(7) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend. Die §§ 30 und 31 des Strafgesetzbuches gelten entsprechend, wenn der Täter zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz handelt.

(8) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

Strafgesetzbuch StGB

§ 202 StGB, Verletzung des Briefgeheimnisses

(1) Wer unbefugt

1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder
2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 (Post- und Fernmeldegeheimnis) mit Strafe bedroht ist.

(2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.

(3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

§ 202 a StGB, Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft..

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b StGB, Abfangen von Daten

(1) Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c StGB, Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 202 d, Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. ...

Auszug aus dem Strafgesetzbuch (StGB)

§ 203 StGB, Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

....

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. ....
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist, anvertraut worden oder sonst bekanntgeworden ist.

Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen

Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) (weggefallen)

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204 StGB, Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 203 Abs. 4 gilt entsprechend

§ 263 a StGB, Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 (Betrug) Abs. 2 bis 7 gilt entsprechend.

§ 269 StGB, Fälschung beweiserheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.

§ 270 StGB, Täuschung im Rechtsverkehr bei Datenverarbeitung

Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich.

§ 303 a StGB, Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

Telekommunikationsgesetz TKG

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an

andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.