Datenschutzrechtliche Herausforderungen für Arztpraxen beim Austausch von Patientendaten

25. Frühjahrstagung der AG Medizinrecht in Mannheim – 28.03.2025

RA Dr. Dominik Nikol

Dominik.Nikol@nikolgoetz.com

Agenda

I. Problemstellung

II. Begriff „Patientendaten“

III. Rechtlicher Rahmen

- Datenschutzrecht
- Strafrecht
- Berufsrecht (Berufsordnungen der Ärzte)

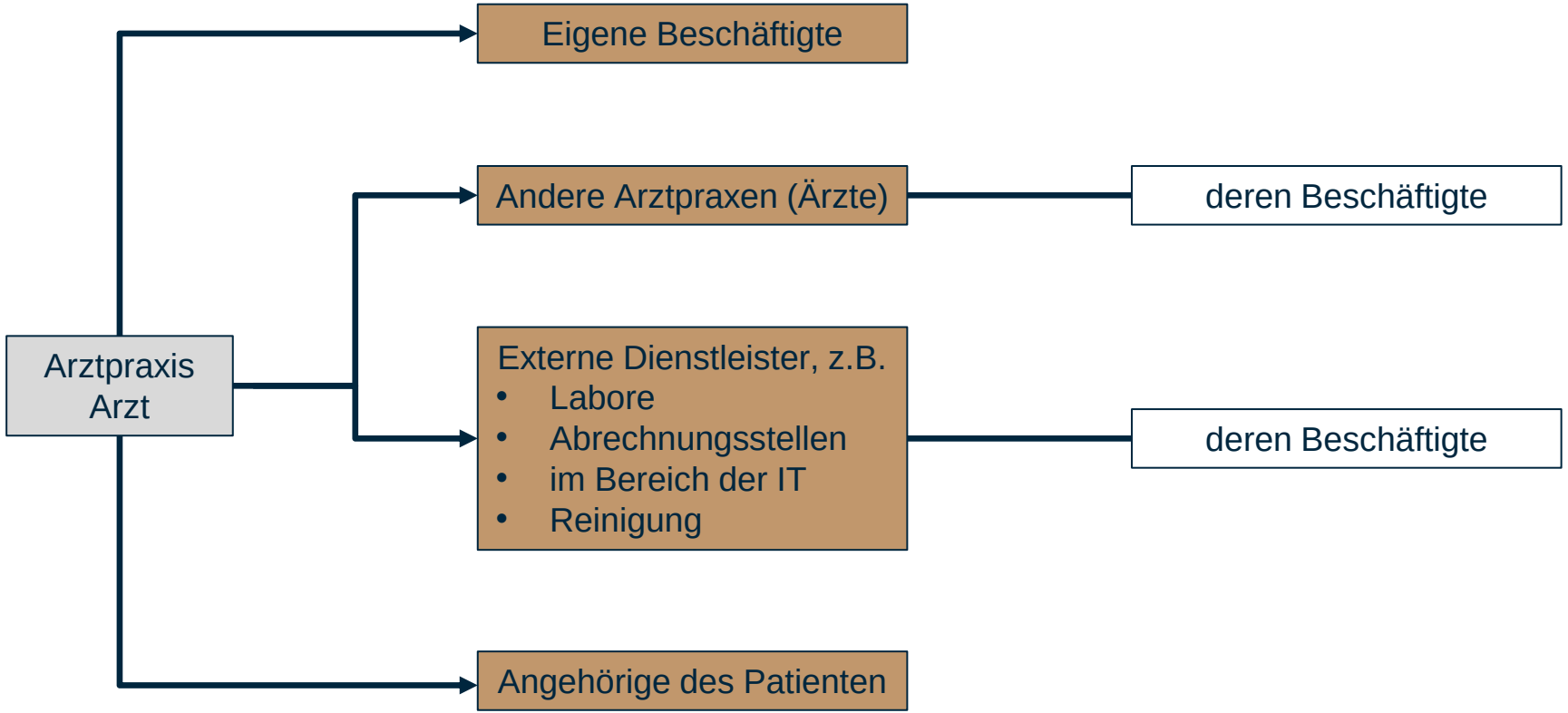
IV. Datensicherheit

V. Zusammenfassung / To-Do‘s

Diskussion (ePA?)

I.
Problemstellung

Eine Arztpraxis (Arzt) gibt Patientendaten an andere Stellen bzw. Personen weiter…



Rechtliche Herausforderungen …

… bestehen insbesondere im Hinblick auf:

- Datenschutzrecht:
  - Datenschutz-Grundverordnung („*DSGVO*“).
  - Bundesdatenschutzgesetz („*BDSG*“).
- Strafrecht:
  - Strafgesetzbuch („*StGB*“).
- Berufsrecht der Ärzte:
  - (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte („*MBO-Ä*“) bzw. entsprechende Bestimmungen der Berufsordnungen der Landesärztekammern.
  - im Folgenden nur Verweise auf MBO-Ä.

II.
Begriff „Patientendaten“

Patientendaten

- Begriff „Patientendaten“ ist nicht gesetzlich definiert.

- Datenschutzrecht:
  - „personenbezogene Daten“ = „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ (Art. 4 Nr. 1 DSGVO).

    ➔ Ist Patient anhand der enthaltenen Information, ggf. mit weiteren Informationen verknüpft, identifizierbar? Berücksichtigung aller Mittel, die von der Arztpraxis oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden können (vgl. ErwG 26 S. 3 DSGVO).
  - „Gesundheitsdaten“ = „Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“ (Art. 4 Nr. 15 DSGVO).

    ➔ EuGH: Weite Auslegung! Mehr als nur ‚medizinische Daten‘. Auch Daten, aus denen mittelbar Rückschlüsse über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand einer Person gezogen werden können.

    ➔ Besondere Datenschutz-Vorgaben für solche sensiblen Daten (Art. 9 DSGVO).

Patientendaten

- Strafrecht (§ 203 StGB – „Verletzung von Privatgeheimnissen“):
  - Offenbarungsverbot für Ärzte in Bezug auf „fremde Geheimnisse“.
  - Offenbarungsverbot bezieht sich auf jede Information, die im Rahmen eines Arzt-Patienten-Verhältnisses entsteht und an der ein sachlich begründetes Interesse besteht.
  - Umfasst sind Tatsachen und Umstände, die sich auf den Gesundheitszustand des Patienten beziehen, sowie Gedanken, Meinungen, Empfindungen, Handlungen und Wissen über familiäre, finanzielle und berufliche Verhältnisse, soweit der Patient an deren Geheimhaltung erkennbar ein Interesse hat.
  - Umfasst ist wohl auch schon Information darüber, dass sich eine Person bei einem Arzt in medizinischer Behandlung befindet.

Patientendaten

- Berufsrecht (§ 9 Abs. 1 MBO-Ä):
  - Eine ärztliche Schweigepflicht besteht in Bezug auf alles was „in [der] Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist“.

➔ **Im Folgenden wird der Begriff „Patientendaten“ als weiter Oberbegriff verwendet, um die verschiedenen Rechtsgebiete abzubilden (einschließlich „Gesundheitsdaten“).**

III.
Rechtlicher Rahmen

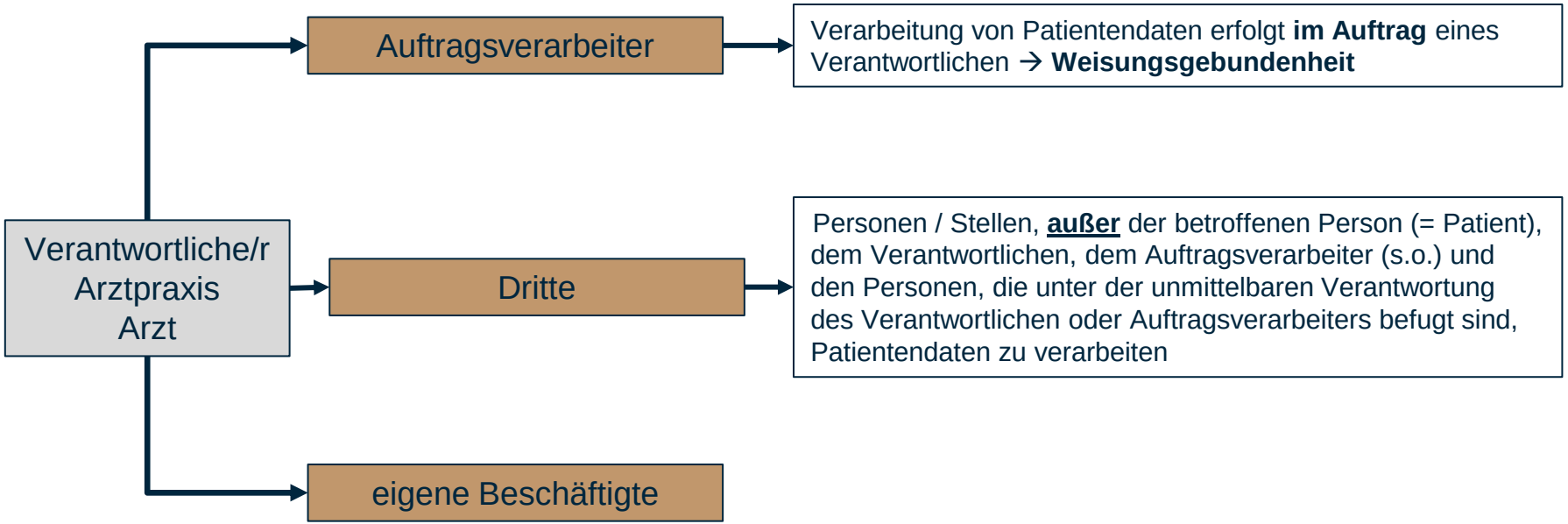
Datenschutzrecht

- Verantwortlichkeit: Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 DSGVO).
  - Je nach Struktur einzelner Arzt oder Arztpraxis.

- Verbotsprinzip mit Erlaubnisvorbehalt (Art. 6 DSGVO): Erfordernis einer Rechtsgrundlage für Verarbeitung personenbezogener Daten für Verantwortliche.
  - Beispiel: „Offenlegung durch Übermittlung“ wie die Weiterleitung von Patientendaten an Dritte; auch bloße Möglichkeit eines Zugriffs eröffnen = jeweils Verarbeitung.

Datenschutzrecht

- Notwendigkeit einer Rechtsgrundlage hängt von datenschutzrechtlicher Rolle des ‚Empfängers' der Daten ab. Empfänger können unterschiedliche Rollen haben:



Überblick über datenschutzrechtliche Rollen

Verantwortliche/r
Arztpraxis
Arzt

Beschäftigte	Auftragsverarbeiter	Dritte
werden Sphäre des Verantwortlichen zugerechnet	z.B. IT-Dienstleister für Hosting / Speichern von Patientendaten	z.B. andere Arztpraxen, Angehörige → grds. alle sonstigen Stellen / Personen
Ausnahme: ‚Exzess‘	agieren als „Mittel“ des Verantwortlichen (h.M.)	
keine weitere RGL für Weitergabe erforderlich	RGL für Weitergabe leitet sich aus der für die Verarbeitung durch den Verantwortlichen ab; keine ‚zusätzliche‘ RGL erforderlich (h.M.)	RGL für Weitergabe erforderlich!
Vertraulichkeits- bzw. Geheimhaltungs-verpflichtung	**AVV nach Art. 28 DSGVO** ***Vertraulichkeits- bzw. Geheimhaltungs-verpflichtung für dessen Beschäftigte***	**RGL im Einzelfall sicherstellen** **Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 DSGVO**

Datenschutzrecht

- Teilweise diskussionswürdig bei Dienstleistern: Weisungsgebundenheit (notwendig für Auftragsverarbeitung)

  Beispiele für umstrittene Konstellationen in der Praxis:
  - Labore (wohl davon abhängig, ob solchen ein Berufsgeheimnisträger vorsteht).
  - private Abrechnungsstellen (wohl vom Umfang der genauen Tätigkeit abhängig).

Datenschutzrecht: Rechtsgrundlagen

Mögliche Rechtsgrundlagen für die Übermittlung von Patientendaten in der Praxis sind:

- Behandlungsvertrag.
  - Soweit Übermittlung zur Durchführung vorvertraglicher Maßnahmen oder zur Erfüllung des Behandlungsvertrags mit Patienten erforderlich ist.
  - Besondere Vorgaben bei „Gesundheitsdaten“: Art. 6 Abs. 1 lit. b i.V.m. 9 Abs. 2 lit. h, Abs. 3 DSGVO i.V.m. § 22 Abs. 1 Nr. 1 lit. b, Abs. 2 BDSG, insbesondere:

    ➔ Verarbeitung nur durch ärztliches Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden.

    ➔ angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen (= Patienten), z.B. Pseudonymisierung vor Übermittlung.

Datenschutzrecht: Rechtsgrundlagen

- Gesetzliche Grundlage.
  - Spezialgesetze, insbesondere Sozialgesetzbücher (z.B. § 294 SGB V zur Übermittlung an Krankenkassen oder § 201 SGB VII an gesetzliche Unfallversicherungen).
- Wahrung lebenswichtiger Interessen.
  - Ausnahmesituationen; Patient ist außer Stande eine Einwilligung abzugeben.
- Überwiegendes berechtigtes Interesse.
  - Geringe praktische Relevanz; bei Gesundheitsdaten nicht anwendbar (Art. 9 DSGVO).
- In allen anderen Fällen: Einwilligung des Patienten (!).
  - freiwillig, bestimmt, informiert, unmissverständliche Willensbekundung, jederzeit widerruflich
  - Praxis: Vorhalten von **Einwilligungsformularen.**

Datenschutzrecht

Weitere Folgen der Verantwortlichkeit, die stets zu beachten sind:

- Grundsatz der Datenminimierung.
- Grundsatz der Zweckbindung.
- Grundsatz der Integrität und Vertraulichkeit (Datensicherheit).
- Informationspflichten ggü. betroffenen Personen (= Patienten)
  - Datenschutzhinweise zur Verfügung stellen.
- ...

Strafrecht

Gemäß § 203 Abs. 1 Nr. 1 Alt. 1 StGB ist es dem einzelnen Arzt verboten, ein fremdes Geheimnis, das ihm anvertraut worden oder sonst bekanntgeworden ist, unbefugt zu offenbaren.

1. Merkmal: „Geheimnis“.

- Letztlich jede Information, die während Arzt-Patienten-Verhältnisses entsteht (*vgl. II.)*.

2. Merkmal: „Offenbaren“.

- Liegt vor, wenn das Geheimnis an eine andere Person gelangt.
  - Ob Information tatsächlich zur Kenntnis genommen wird, ist irrelevant; Möglichkeit der Kenntnisnahme ist ausreichend, z.B. durch eine potentielle Zugriffsmöglichkeit (ggf. Beschäftigte von Dienstleistern).
- Einschränkung durch § 203 Abs. 3 S. 1 StGB.
  - Erlaubnistatbestand für „berufsmäßig tätigen Gehilfen“ und „zur Vorbereitung auf den Beruf tätigen Personen“ (z.B. med. Fachangestellte oder Beschäftigte im Sekretariat).

Strafrecht

- Einschränkung durch § 203 Abs. 3 S. 2 StGB.
  - Sondertatbestand für sonstige Personen, die „an der beruflichen (…) Tätigkeit mitwirken“ (z.B. externe Dienstleister für IT, Aktenvernichtung oder Schreibdienst).
  - Offenbarung zulässig, soweit dies für die Inanspruchnahme der Tätigkeit der mitwirkenden Personen erforderlich ist.
  - Zusatzvoraussetzung: Geheimhaltungsverpflichtung (§ 203 Abs. 4 StGB).
  - Geheimhaltungsverpflichtung muss im Hinblick auf weitere Personen (z.B. Sub-Dienstleister) sichergestellt sein ➔ „Kette“ der Geheimhaltungsvereinbarung bis hin zum (behandelnden) Arzt muss gewährleistet sein.
  - Ansonsten ggf. eigene Strafbarkeit des Arztes nach § 203 Abs. 4 Nr. 1 StGB.
  - Verstößt Person gegen die ihr auferlegte Geheimhaltungsverpflichtung kommt eine Strafbarkeit aus der sog. abgeleiteten Verschwiegenheitspflicht nach § 203 Abs. 4 Nr. 2 StGB in Betracht.

Strafrecht

3. Merkmal: „unbefugt“

- Insbesondere relevant, wenn es sich auf Seiten des Empfängers nicht um eine Person handelt, die an der beruflichen Tätigkeit des Arztes „mitwirkt“ (z.B. „Exzess“, oder Dritter).
- Befugnis kann aufgrund von Spezialgesetzen (z.B. Krankenkassen, Unfallversicherung), der Vorlage einer Bevollmächtigung oder des Vorliegens eines Einverständnisses des Patienten bestehen.
  - Bei Einverständnis des Patienten: Entbindung von Schweigepflicht erforderlich.

Nach dem sog. „Zwei-Schranken-Prinzip“ muss dieses Einverständnis gesondert zu etwaigen datenschutzrechtlichen Einwilligungen eingeholt werden.

- Abfrage von Einverständnis und der datenschutzrechtlichen Einwilligung in einer einheitlichen Erklärung ist aber möglich.

Berufsrecht

- Gem. § 9 Abs. 3 MBO-Ä sind Ärzte verpflichtet die Beschäftigten sowie Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, „über die gesetzliche Pflicht zur Verschwiegenheit“ zu belehren. Dies ist schriftlich festzuhalten.

- Gem. § 9 Abs. 4 MBO-Ä müssen Beschäftigte von Dienstleistern und sonstige mitwirkende Personen in Schriftform zur Geheimhaltung verpflichtet werden.

Berufsrecht

- Ärzte, die gleichzeitig oder nacheinander denselben Patienten behandeln, sind untereinander von der Schweigepflicht insoweit befreit, als dass das Einverständnis des Patienten „vorliegt oder anzunehmen“ ist (§ 9 Abs. 5 MBO-Ä).
  - Umfang dieser „Befugnis“ zur Offenbarung in Bezug auf § 203 StGB ist strittig.
  - Datenschutzrecht kennt grundsätzlich keine „mutmaßliche Einwilligung“, gerade bei Gesundheitsdaten ist „ausdrückliche“ Einwilligung erforderlich (Art. 9 Abs. 2 lit.a DSGVO); möglich jedoch Berücksichtigung im Rahmen des geschlossenen Behandlungsvertrags.
  - In der Praxis restriktive Handhabung des mutmaßlichen Einverständnisses vorzugswürdig.
- Die berufsrechtlichen Bestimmungen zur Belehrung und Verpflichtung von mitwirkenden Personen in Schriftform geht im Ergebnis über die Anforderungen des § 203 StGB hinaus.

IV.
Datensicherheit

Datensicherheit: „Wie“ der Übermittlung

- Datenschutzrecht: Datensicherheit ist vor allem durch Implementierung sog. „technischer und organisatorischer Maßnahmen“ sicherzustellen (Art. 32 DSGVO).
  - Vorschrift verpflichtet sowohl Verantwortliche als auch Auftragsverarbeiter.
  - Risikobasierter Ansatz.
  - Angemessenheit von Maßnahmen ist im Einzelfall unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen (= Patienten) zu ermitteln.

Datensicherheit: „Wie“ der Übermittlung

- Vorliegen eines Berufsgeheimnisses ist regelmäßig Indiz für ein hohes datenschutzrechtliches Risiko → hohe Anforderungen an die Datensicherheit.
- Niedriges Niveau der Datensicherheit:
  - einfache E-Mail.
  - Fax.
- Grundsätzlich höheres Niveau der Datensicherheit:
  - Ende-zu-Ende-Verschlüsselung.
  - persönliche Übergabe.
  - Nutzung gesondert abgesicherter Umgebungen.
- Offen: Inwieweit könnte ein Patient in ein niedrigeres Datensicherheitsniveau einwilligen?

Darf ich Gesundheitsdaten wie Arztberichte oder Röntgenbilder per Telefax oder E-Mail senden oder anfordern?

Eine unverschlüsselte E-Mail oder ein Telefax ist vergleichbar mit einer Postkarte, welche leicht von Dritten mitgelesen werden kann. Dies kann eine unbefugte Offenbarung von Patientengeheimnissen darstellen. Im Gesundheitsbereich enthalten alle E-Mails automatisch einen Bezug zu besonderen Kategorien personenbezogener Daten (Gesundheitsdaten). Für die Übermittlung dieser Daten ist zum einen entweder eine Rechtsgrundlage oder die Einwilligung der Betroffenen erforderlich, zum anderen hat die oder der Verantwortliche angemessene technisch-organisatorische Maßnahmen zu treffen, welche die Sicherheit der Übermittlung gewährleisten. Gesundheitsdaten dürfen daher nur mit einem, dem aktuellen Stand der Technik entsprechenden, **sicheren Verschlüsselungsverfahren** übermittelt werden.

Datenschutzgerechte Übermittlungswege sind unter anderem: Persönliche Übergabe, Versand per Brief, hinreichend inhaltsverschlüsselte E-Mail (Ende-zu-Ende Verschlüsselung bzw. per Gateway-Lösung) oder die Inanspruchnahme gesonderter abgesicherter Umgebungen (z.B. in einem Virtuellen-Privaten-Netzwerk (VPN), die Kommunikation im Medizinwesen (KIM) oder der Messenger der Telematik Infrastruktur).

Weitere Informationen bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf dessen Homepage www.bsi.bund.de.

https://www.lfd.niedersachsen.de/faq/gesundheitsbereich/faq-gesundheitsbereich-und-datenschutz-229071.html

Stand Januar 2024

V.
Zusammenfassung / To-Do‘s

Beschäftigte von Arztpraxen (Ärzten)

- Belehrung über gesetzliche Pflicht zur Verschwiegenheit in Schriftform.
  - vgl. § 9 Abs. 3 MBO-Ä
- Grundsätzlich Verpflichtung zur Vertraulichkeit bzw. Geheimhaltung in Bezug auf personenbezogene Daten in Schriftform.
  - vgl. Art. 5 Abs. 1 lit. f, Art. 32, Abs. 1 und Abs. 4 iVm Art. 5 Abs. 2 DSGVO.
  - vgl. Art. 9 Abs. 2 lit. h, Abs. 3 DSGVO iVm § 22 Abs. 1 lit. b BDSG.
- Beschäftigte dürfen nur Zugriff auf die für ihre jeweilige Tätigkeit erforderlichen Patientendaten haben → Sicherstellen durch entsprechende Maßnahmen (TOMs).
  - vgl. Art. 5 Abs. 1 lit. f, Art. 32, Abs. 1 und Abs. 4 DSGVO.
  - z.B. individuell festgelegte Rechte für Zugriff auf bestimmte Patientenakten durch IT-Einstellungen oder abschließbare Schränke (z.B. Praxisgemeinschaften mit den jeweiligen Ärzten fest zugewiesenem Personal).
  - z.B. individuell festgelegte Rechte für Zugriff auf bestimmte Teile von Patientenakten durch IT-Einstellungen oder besondere Aktenführung.

Auftragsverarbeiter von Arztpraxen (Ärzten)

- Datenschutzrechtliche Rolle von Dienstleistern im Einzelfall prüfen.
- Auftragsverarbeiter, die an beruflichen Tätigkeiten mitwirken, dürfen eingesetzt werden, sofern Arztpraxis (Arzt) eine Rechtsgrundlage für die zugrundeliegende Verarbeitung vorweisen kann (h.M.) → die Rechtsgrundlage ist für die einzelne Verarbeitungstätigkeit zu ermitteln und dokumentieren.
  - vgl. Art. 5 Abs. 1 lit. a, Art. 6, Art. 9 DSGVO.
- Auftragsverarbeiter darf nur Zugriff auf die für die jeweilige Tätigkeit erforderlichen Patientendaten haben → Sicherstellen durch entsprechende Maßnahmen (TOMs).
  - vgl. Art. 5 Abs. 1 lit. f, Art. 32, Abs. 1 und Abs. 4 DSGVO.
  - vgl. § 203 Abs. 3 S. 2 StGB.
  - Konkrete Maßnahmen sind abhängig von Tätigkeit des Auftragsverarbeiters für Arztpraxis.
- Abschluss eines Auftragsverarbeitungsvertrags.
  - vgl. Art. 28 Abs. 3 DSGVO.

Auftragsverarbeiter von Arztpraxen (Ärzten)

- (Schriftliche) Vereinbarung mit jedem Auftragsverarbeiter, dass dessen Beschäftigte, die Zugriff auf Patientendaten haben oder haben könnten, zur Vertraulichkeit bzw. Geheimhaltung verpflichtet werden (!).
  - vgl. Art. 28 Abs. 3 lit. b und Art. 9 Abs. 2 lit. h, Abs. 3 DSGVO iVm § 22 Abs. 1 lit. b BDSG.
  - vgl. § 203 Abs. 4 Nr. 1 StGB, § 9 Abs. 4 MBO-Ä.
- (Schriftliche) Vereinbarung, dass weitere Sub-Auftragnehmer bzw. dessen Beschäftigten zur ebengleichen Vertraulichkeit bzw. Geheimhaltung verpflichtet werden.
  - vgl. Art. 28 Abs. 3 lit. b und Art. 9 Abs. 2 lit. h, Abs. 3 DSGVO iVm § 22 Abs. 1 lit. b BDSG.
  - vgl. § 203 Abs. 4 Nr. 1 StGB, § 9 Abs. 4 MBO-Ä.
- Sicherstellen eines angemessenen Niveaus der Datensicherheit beim Dienstleister.
  - vgl. Art. 32 DSGVO.

Andere externe Stellen und Personen („Dritte“)

- Datenschutzrechtliche Rolle als Verantwortliche im Einzelfall prüfen.
- Dritte dürfen auf Patientendaten nur Zugriff haben (einschließlich Übermittlung), sofern Arztpraxis (Arzt) eine Rechtsgrundlage vorweisen kann → die Rechtsgrundlage ist zu ermitteln und dokumentieren.
  - vgl. Art. 5 Abs. 1 lit. a, Art. 6, Art. 9 iVm Art. 5 Abs. 2 DSGVO.
- Sofern Rechtsgrundlage die Einwilligung/Einverständnis des Patienten ist:
  - Anforderungen an datenschutzkonforme Einwilligungen einhalten, insbesondere Angabe der Empfänger der Patientendaten, vgl. Art. 6 Abs. 1 lit. a, Art. 4 Nr. 11, Art. 7 DGSVO.
  - Möglichkeit von Widerrufen der Einwilligung mitberücksichtigen, vgl. Art. 7 Abs. 3 DSGVO.
  - Zusätzlich: Einverständnis in die Entbindung von ärztlicher Schweigepflicht, vgl. § 203 Abs. 1 Nr. 1 Alt. 1 StGB, § 9 Abs. 1, Abs. 2 MBO-Ä; ggf. Ausnahme bei Übermittlung an andere Ärzte vgl. § 9 Abs. 4 MBO-Ä (str.).
- Sicherstellen eines angemessenen Niveaus der Datensicherheit.
  - vgl. Art. 32 DSGVO.

NIKOL & GOETZ

Vielen Dank!

Diskussion

NIKOL & GOETZ

Kontakt:

Dominik.Nikol@nikolgoetz.com
oder über LinkedIn