DR. THOMAS GIESEN

DATENSCHUTZBEAUFTRAGTER DER DEUTSCHEN HAUSÄRZTEVERBÄNDE

DR. THOMAS GIESEN · PALAISPLATZ 3 · 01097 DRESDEN

Datenschutz in der Arztpraxis

Da ziehen in letzter Zeit Propheten durch das Land und verwirren die Ärzteschaft mit allerlei Aufgeregtheiten zum Datenschutz. Deshalb muss dringend für Sachlichkeit gesorgt werden. Leider schweigen die Ärztekammern noch immer: Beim Datenschutz in der Arztpraxis erwarten uns grundsätzliche Erleichterungen in der rechtlichen Systematik, aber – wie leider immer – auch mehr Bürokratie.

Ab 25. Mai 2018 wird es **Änderungen im Datenschutzrecht** geben: Die EU hat nach langen Beratungen eine neue, letztlich einfachere und bessere Regelung für den ärztlichen Bereich beschlossen. Wir bemerken leider, dass nun viele Wichtigtuer und Gschaftlhuber die Gelegenheit nutzen, ins Geschäft zu kommen, oder für rechtspolitische Unordnung zu sorgen. Vieles wird sich in der Praxis der Datenschutzbehörden noch entwickeln. Dennoch zur Klärung und Versachlichung einige Klarstellungen bereits jetzt:

Das Datenschutzrecht in der ärztlichen Berufsausübung ist im Kern die **Wahrung der ärztlichen Schweigepflicht**. Der Umgang mit Patientendaten ist deshalb beschränkt und stark reguliert: Informationen über Patienten dürfen nur erhoben, genutzt und mitgeteilt werden, wenn das zur Erfüllung des Behandlungsvertrags geeignet und erforderlich ist. Diese Selbstverständlichkeit ist jedem Arzt eigentlich geläufig.

Der notwendige Umgang mit Patientendaten im elektronischen Arztinformationssystem oder Praxisverwaltungssystem ist folglich zu Recht vom Datenschutzrecht beherrscht.

Zunächst: Man sollte **nur geprüfte und handelsübliche Hard- und Software** nutzen. Übermittlungswege müssen "dicht" also verlässlich gesichert sein; die Daten sind zum Transport grundsätzlich zu verschlüsseln. Der HZV-Online-Key und die Dateiverschlüsselung entsprechen bereits dem künftigen technischen Standard. Auch die weiteren Angebote oder Empfehlungen der HÄVG werden ihm genügen.

1. Interne und externe Helfer: Belehrungspflicht

Rechtsgrundlage für die Befugnis, im Praxis-Team und gemeinsam mit anderen Leistungserbringern, aber auch Administratoren, Abrechnern und Leistungsträgern mit Patientendaten umzugehen, also, genau genommen, die Schweigepflicht zu brechen, ist künftig **Art. 9** der neuen, direkt und wie ein deutsches Gesetz geltenden **EU-Datenschutz-Grundverordnung** (DS-GVO); sie wird gelegentlich ergänzt durch das **völlig neue Bundesdatenschutzgesetz** (BDSG). Für die Behandlung von Patienten und die sonstige Erbringung von ärztlichen Versorgungsleistungen (einschließlich Vorsorge, Nachsorge und Verwaltung) gilt Art. 9 Abs. 2 Buchstabe h in Verbindung mit Abs. 3 DS-GVO, vorausgesetzt, alle eingesetzten Personen stehen unter der ärztlichen Schweigepflicht. Für die Abrechnung (Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen) gilt Art. 9 Abs. 2 Buchstabe f.

Diese Teambildung ist erleichtert, denn **§ 203 Strafgesetzbuch**, die gesetzliche Rechtsgrundlage für die ärztliche berufliche Schweigepflicht, wurde um **"sonstige Personen"** erweitert: Neben seinen Praxismitarbeitern darf der Arzt – nun endlich klar geregelt – betriebsfremde Helfer einsetzen, etwa Administratoren zur Pflege seiner Hard- und Software, aber auch Abrechnungsstellen, ohne die Einwilligung der Patienten einholen zu müssen.

Alle seine Helfer, die angestellten und die externen, muss der Arzt allerdings auf ihre berufliche Schweigepflicht **belehren**: In der Tat werden durch § 203 Abs. 3 Strafgesetzbuch künftig auch die berufsfremden Helfer, die der Arzt mit Hilfstätigkeiten beauftragt, unter das ärztliche Berufsgeheimnis gestellt, wie das bei seinen Angestellten schon jetzt der Fall ist. Denn auch die fremden Helfer können, gelegentlich auch unbeabsichtigt, Angaben über die Patienten zur Kenntnis nehmen; sie "verarbeiten" also "Patientendaten".

Diese Belehrung muss der Arzt nachweisen können; am besten gewöhnt man sich an, in der Arztpraxis ein Buch zu führen, in dem solche fremden Helfer (für die das Routine wird) unterschreiben, auf die gesetzliche Schweigepflicht nach § 203 Abs. 3 StGB und die Strafbarkeit jedes zweckwidrigen Umgangs mit Patientendaten belehrt worden zu sein; Datum, Unterschrift, fertig.

Bei Verrechnungsstellen sollte der Arzt deren Selbstverpflichtung abfordern, wenn sie nicht ohnehin in den Verträgen erklärt wird, wie das in den HZV-Verträgen natürlich geschieht.

Kann der Arzt diese Belehrungen oder Selbstverpflichtungen nicht nachweisen und wird einer dieser Helfer – wie der Teufel es will – wegen leichtfertigem Umgang mit dem Arztgeheimnis – an dem er ja künftig teilnimmt – bestraft, dann wird der Arzt ebenfalls bestraft (§ 203 Abs. 4 Nr. 1 StGB).

Man sieht, die Rechtsordnung nimmt nach wie vor das ärztliche Berufsgeheimnis ernst, lockert aber die Möglichkeiten, Dritte als Helfer einzubeziehen. Das ist angesichts der Digitalisierung, Spezialisierung und Arbeitsteilung der ärztlichen Berufswelt eine positive gesetzliche Regelung. Jeder Patient vertraut sich seinem Arzt ganz an; würde er befürchten müssen, dass seine Daten aus dem Praxisverwaltungssystem in falsche Hände geraten oder berufsfremd genutzt werden, wäre das für den ärztlichen Berufsstand – das Berufsethos ist für das Ansehen und für den Behandlungserfolg entscheidend – ein Fiasko.

Die Vorkehrungen durch Belehrung betonen, dass es der Arzt ist, der seine auch der Praxis nicht direkt zugehörigen Helfer aussucht und belehrt. Der Arzt bleibt letztlich der Verantwortliche. Das stärkt den Berufsstand.

2. In der Regel kein Datenschutzbeauftragter in der Arztpraxis

Die normale Arztpraxis, also der niedergelassene Arzt, und die üblichen Kooperationsformen von Ärzten, etwa auch kleinere MVZ, sind künftig nicht verpflichtet, einen eigenen betrieblichen Datenschutzbeauftragten zu bestellen.

Diese Pflicht gilt allenfalls für große Einheiten, in denen eine "umfangreiche" Verarbeitung von Gesundheitsdaten (Art. 37 Abs. 1 Buchstabe c DS-GVO), also von Informationen über Patienten, stattfindet. Was "umfangreich" ist, wird leider erst künftig auf EU-Ebene (und nicht nur für Deutschland) geklärt. Wir rechnen fest damit, dass dann auch festgelegt werden wird, ob und wann größere MVZ und andere "Ärzte-Unternehmen" einen eigenen Datenschutzbeauftragten zu bestellen haben. Diese Rechtsentwicklung sollten die betroffenen Unternehmen in Ruhe abwarten.

Einzelheiten:

a) Art. 37 Abs. 1 Buchstabe c DS-GVO verpflichtet Ärzte als Verantwortliche nur dann zur Bestellung eines eigenen Datenschutzbeauftragten, wenn ihre **"Kerntätigkeit"** (engl.: "core activities") in der "umfangreichen Verarbeitung" (engl: "on a large score") von Gesundheitsdaten besteht. Die Kerntätigkeit bezieht sich (sprachlich nur annähernd richtig) auf die "Haupttätigkeit", wie es im Erwägungsgrund 97 Satz 1 lautet. Als anderes Wort für die Kerntätigkeit könnte man auch sagen: das "zentrale berufliche Anliegen", der "Zweck der Tätigkeit" oder kurz der "Beruf im eigentlichen Sinn". So richtig verstanden ist die Kerntätigkeit eines Arztes die ärztliche Behandlung und Gesundheitsversorgung; die Verarbeitung der dabei anfallenden Patientendaten ist nur eine sich daraus ergebende (gesetzlich und vertraglich angeordnete, aber eben nicht zum Kern gehörende, nicht das Berufsbild zentral prägende) Folge der Behandlung oder eine Voraussetzung für die Fortsetzung der Behandlung, nicht aber die Kerntätigkeit.

Die in § 630f BGB angeordnete Dokumentationspflicht der Ärzte führt zwar zu einer durchaus wichtigen (aber eben nicht das Kernanliegen der ärztlichen Berufsausübung ausmachenden), heute meist automatisierten Datenverarbeitung: Die Daten der Patienten werden digital oder zumindest in Dateien gespeichert und verarbeitet. Diese Dokumentationspflicht ist aber eine berufliche **Nebenpflicht**, die sich aus Gesetz und Vertrag ergibt; siehe z. B. Palandt/Weidenkaff, Kommentar zum BGB, 75. Auflage 2016, § 630f Rn. 1). Solche Nebenpflichten sind für die Bestellung eines Datenschutzbeauftragten ausdrücklich unbeachtlich, siehe Erwägungsgrund 97 Satz 2.

b) Etwas anderes ist die Pflicht eines Rechenzentrums (wie die HÄVG RZ GmbH) oder eines Abrechnungsunternehmens (PVS): Sie sind, wenn auch als Auftragnehmer, im Kerngeschäft mit der Verarbeitung von Patientendaten befasst; dort ist ein Datenschutzbeauftragter aus guten Gründen zu bestellen; er wird auch genug Arbeit finden.

c) Soweit § 22 Abs. 2 Nr. 4 BDSG (neu) angemessene und spezifische Maßnahmen zur Wahrung des Persönlichkeitsrechts der betroffenen Person (das ist im Fall von Gesundheitsdaten der Patient) vorzusehen vorschreibt, "**kann** dazu insbesondere gehören", einen Datenschutzbeauftragten zu benennen. Dieses "kann" ist eben – auch anders als etwa ein "soll" in der deutschen Gesetzessprache, wenn Adressat des Gesetzes eine öffentliche Stelle ist – kein "muss", sondern Ausdruck der Benennungsmöglichkeit, folglich keine Vorschrift, die eine Bestellung verpflichtend vorschreibt.

Das wird durch die Gesetzesmaterialien bestätigt: Ursprünglich sah der Gesetzesentwurf der Bundesregierung in einem gesonderten Absatz 2 Satz 3 zu § 22 BDSG (neu) vor, dass die besonderen Vorkehrungen des gesamten Absatzes 2 überhaupt nicht gelten sollten, wenn die ärztliche Schweigepflicht (einschl. des Personals und "sonstiger Personen", siehe § 203 Abs. 3 StGB neu) gilt. Diese Ausnahme ist nur deshalb auf Vorschlag des Bundesrates gestrichen worden, weil – so BT Drs. 18/12144 Seite 4 – das der Klarstellung dient und den Eindruck vermeidet, dass für alle Datenverarbeitungen nach § 22 Abs. 1 Nummer 1 Buchstabe b BDSG keine angemessenen und spezifischen Maßnahmen zu ergreifen sind. Das ist richtig, denn u. a. auch Ärzte müssen ihre Daten besonders schützen und sichern. Es bleibt aber dabei, dass die Vorschrift keine Pflicht des Arztes statuiert, einen betrieblichen Datenschutzbeauftragten zu bestellen.

d) Alles andere, was zur Bestellung von Datenschutzbeauftragten gelegentlich geschrieben und behauptet wird, mag "datenschutzfreundlich" oder gar "ideologisch gestreamt" (oder gar geschäftstüchtig) sein, ist jedoch von den Rechtsvorschriften – Datenschutz ist Teil der Rechtsordnung, nicht mehr und nicht weniger – nicht gedeckt: Soweit § 38 Abs. 2 BDSG (neu) die Bestellung eines eigenen Datenschutzbeauftragten ergänzend auch dann vorschreibt, wenn der Verantwortliche "in der Regel mindestens 10 Personen **ständig** (warum hat der deutsche Gesetzgeber das ausdrücklich so betont, wenn es dann in Teilen der Literatur unerwähnt bleibt? Anm. d. Verf.) mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen", so beschreibt dies ein Maß, das in der Realität einer Arztpraxis oder ärztlichen Kooperation **praktisch kaum vorkommt**.

Die **Anzahl der Mitarbeiter** – das ist ein Maßstab, den Deutschland traditionell gern nach vorn schiebt, um dem Berufsstand der betrieblichen Datenschutzbeauftragten gefällig zu sein – trifft eigentlich keine wirklich maßgebliche Aussage dazu, ob das Persönlichkeitsrecht etwa des einzelnen Patienten besonderen Gefährdungen ausgesetzt ist; dieser Maßstab erscheint folglich nicht wirklich verhältnismäßig zu sein. Zudem weicht dieser Maßstab als völlig neu hinzugenommenes Entscheidungskriterium – es handelt sich eben nicht um eine Ergänzung, sondern um einen gänzlich anderen Problemansatz – von der (nur mittelbaren) Öffnungsklausel in Art. 37 Abs. 4 DS-GVO für den nationalen Gesetzgeber ab; mit den Kommentatoren des Bundesinnenministeriums (Gierschmann u. a. Art. 37 Rn. 106) ist daher insofern an der Kompetenz des deutschen Gesetzgebers zu zweifeln.

Ferner schreibt § 38 BDSG die Bestellung eines Datenschutzbeauftragten dann vor, wenn der Verantwortliche Verarbeitungen vornimmt, die der Pflicht einer vorherigen **Datenschutz-Folgen-Abschätzung** nach Art. 35 DS-GVO unterliegen. Das ist etwa bei umfangreichen Forschungsvorhaben oder besonders risikoreichen oder heimlich überwachenden Verarbeitungsformen oder bei dem Einsatz neuer, noch nicht praxiserprobter Verarbeitungstechniken oder bei besonders umfangreicher Verarbeitung von Gesundheitsdaten der Fall. Mit der üblichen Tätigkeit von Ärzten sind solche Risiken nicht verbunden. Bevor Krankenhäuser oder ärztliche Abrechnungs-Rechenzentren neue Verarbeitungsverfahren mit auffällig sensitiven und innovativen Methoden einrichten, ist eine Datenschutzfolgeabschätzung geboten und selbstverständlich. Es versteht sich, dass dann die Risiken eines Angriffs oder eines Missbrauchs genau abzuchecken und konsequent auszuschließen sind. Für den "normalen" Arzt ist das aber nicht einschlägig.

3. Interne Dokumentation: Verarbeitungsverzeichnis

In der Arztpraxis ist ab 25.05.2018 ein **Verarbeitungsverzeichnis nach Art. 30 DS-GVO zu führen**: Zwar ist keine Form vorgeschrieben, jedoch empfiehlt sich die Schriftform.

Name und Erreichbarkeit des Praxisinhabers (evtl. seines Vertreters), Zwecke der Verarbeitung, Beschreibung der Datenkategorien und Betroffenen, Pseudonymisierung, regelmäßige Empfänger der Daten, Fristen der Löschung, prägnante Beschreibung der technischen und organisatorischen Schutzmaßnahmen.

Beispiel für ein **Verarbeitungsverzeichnis**:

*- **Verantwortlich** für die Verarbeitung der Patientendaten ist der Praxisinhaber: Name, Titel, Facharzt für Allgemeinmedizin, Adresse, Telefonnummer, E-Mail-Adresse.*

- Ein ständiger Vertreter in der Arztpraxis ist nicht vorhanden; bzw. Name des ständigen Vertreters.

*- Im **Praxisverwaltungssystem** (Hersteller, Vertreiber, Betreuer: Name und Adresse) werden Patientendaten zum Zweck der ärztlichen Versorgung – auch von beteiligten Leistungserbringern untereinander – und zur gesetzlichen oder vertraglichen Abrechnung erhoben, gespeichert, verarbeitet und übermittelt. Die Erhebung erfolgt beim Patienten oder von anderen Leistungserbringern in grundsätzlicher Kenntnis des Patienten. Ausnahmen werden dokumentiert.*

*- Regelmäßige **Übermittlungen** erfolgen an andere Leistungserbringer entsprechend dem individuellen Verlauf des Behandlungsgeschehens.*

*- Ferner erfolgen Übermittlungen zur Abrechnung der **Kollektivversorgung** an die Kassenärztliche Vereinigung (Adresse; Telefonnummer und E-Mail-Adresse; dortiger Datenschutzbeauftragter: Adresse; Telefonnummer und E-Mail-Adresse) bzw. die jeweilige Krankenkasse des Patienten*

*- oder in der **Selektivversorgung (HZV)** an die HÄVG RZ GmbH, Edmund-Rumpler-Straße 2, 51149 Köln, Tel. 02203 5756-1111; Datenschutzbeauftragter: Dr. Thomas Giesen, gleiche Erreichbarkeit.*

*- Für **Privatpatienten** gilt u. U.: Wir lassen unsere Abrechnungen in der PVS (Name, Adresse, Datenschutzbeauftragter: Name und Adresse) herstellen und übermitteln ausschließlich zu diesem Zweck dorthin Ihren Namen, Ihre Adresse, abrechnungsrelevante Daten, z. B. Diagnosen, Befunde, Medikationen, erbrachte Leistungen, Krankheitsverläufe. Die PVS steht unter der gleichen Schweigepflicht wie wir selbst. Die Gesundheitsdaten werden dort nach vier Jahren gelöscht; die Adressdaten der Patienten werden 10 Jahre aufbewahrt; nach vier Jahren werden sie gesperrt.*

*- **Rechtsgrundlagen** der Verarbeitung sind der Behandlungsvertrag zwischen Arzt und Patient sowie das Gesetz (Art. 6 Abs. 1 Buchstabe b, Art. 9 Abs. 2 Buchstabe f und Buchstabe h in Verbindung mit Abs. 3 DS-GVO und § 295 und § 295a SGB V, sowie (selten) gesetzliche Meldepflichten.*

Rechte der betroffenen Patienten

- Auskünfte an Betroffene oder ihre Vertreter werden wunschgemäß auch einmalig durch Abschriften erteilt; auch die Rechte auf Berichtigung nach Art. 16, auf Löschung nach Art. 17 und auf Einschränkung der Verarbeitung/Sperrung nach Art. 18 DS-GVO werden erfüllt.

Aufbewahrungsdauer

- Datensperrung erfolgt nach vier Jahren, Datenlöschung erfolgt nach 12 Jahren; Röntgenaufnahmen werden nach 30 Jahren vernichtet.

Datensicherheit

- Die Daten werden in Akten sowie im automatisierten elektronischen Praxisverwaltungssystem verarbeitet. Die Patientenakten werden sicher verschlossen; die getroffenen technischen und organisatorischen Maßnahmen für den Schutz des elektronischen Praxisverwaltungssystems entsprechen dem Stand der Technik und umfassen insbesondere (nicht Zutreffendes streichen):

- *Den physischen Zutrittsschutz zu Serversystemen und Endgeräten, hier insbesondere zu Systemschnittstellen durch abschließbare Türen mit Sicherheitsschlössern*
- *Die Nutzung von ausfallsicheren bzw. redundanten Komponenten (z. B. Festplatten-Verbund-Konfigurationen/RAIDs, Netzteilen) sowie ein Schutz gegen plötzlichen Stromausfall und Spannungsspitzen insbesondere für Server-Systeme*
- *Den Schutz gegen unbefugten Zugriff auf das Netzwerk durch Überwachung von Netzwerk-Anschlüssen / physisches Abklemmen von nicht genutzten Anschlüssen / Verschlüsselung von Wireless-LAN-Netzen mittels aktueller Verfahren / ...*
- *Die Aufstellung der Bildschirme dergestalt, dass die Einsichtnahme von Daten durch Unbefugte nicht (ohne weiteres) möglich ist,*
- *Die Einrichtung von personengebundenen Zugriffsberechtigungen sowie die Aktivierung des Zugriffsschutzes mittels komplexem Passwort (mind. 10 Stellen; Kombination aus Ziffern, Buchstaben, Sonderzeichen; Wechsel alle x Monate; nicht gleichlautend zum Benutzernamen; nicht aus einem Wörterbuch stammend; ...) / Schlüsselkarte / Biometrie-Scanner*
- *Eine automatische Sperre der Verarbeitungsoberfläche nach 5 / 10 / 15 Minuten Inaktivität und der Aufforderung zur erneuten Authentifizierung mittels o. g. Verfahren (komplexem Passwort / Schlüsselkarte / Biometrie-Scanner)*
- *Eine automatische Sperre der Anmeldemöglichkeit für die Dauer von fünf Minuten nach 10 aufeinander folgenden, erfolglosen Anmeldeversuchen mittels des o. g. Authentifizierungsverfahrens*
- *Die regelmäßige und zeitnahe Aktualisierung der eingesetzten Hard- und Software (Netzwerk-Geräte, Betriebssystem, Standard-Büro-Software, Systemtools, etc.) durch Einspielen von Sicherheitsupdates*

- *Die Einrichtung, regelmäßige Aktualisierung von Programmen zum Schutz vor Malware („Anti-Viren-Software") sowie die zyklische Durchführung von Prüfläufen auf den geschützten Systemen*
- *Eine Absicherung des Internetübergangs mittels*
    - *restriktiver Firewall-Regeln, insb. dem ausschließlichen Verbindungsaufbau aus dem internen Netzwerk heraus*
    - *die Einschränkung der Internetnutzung auf ausgewählte Endgeräte / ausgewählte Seiten / durch Blockieren von unerwünschten Seiten / die inhaltliche Prüfung auf schadhaften Code im Internetverkehr*
- *Eine regelmäßige Sicherung der Daten auf einem vom zentralen Server physisch getrennten Medium, welches insbesondere gegen physische Bedrohungen wie Brand, Wasser, Diebstahl, etc. gesichert gelagert wird.*

Merke: Das Verarbeitungsverzeichnis ist bei sachlichen Änderungen zu aktualisieren.

4. Informationspflicht des Arztes gegenüber dem Patienten

Es wird eine Informationspflicht eingeführt. Sie bezieht sich – siehe dazu die Art. 13 und 14 DS-GVO:

- auf die Person des Verantwortlichen
- den Zweck und die Rechtsgrundlage der Datenverarbeitung
- die Kategorien der Daten (Gesundheitsdaten)
- die (Kategorien der) Empfänger der Daten
- die Zeit der Speicherung
- die Rechte des Betroffenen auf Auskunft, Berichtigung und Löschung oder Sperrung und
- das Recht auf Beschwerde bei der Aufsichtsbehörde.

Diese Information ist jedoch nicht erforderlich und unterbleibt, wenn und soweit der Patient bereits über die Information verfügt (Art. 13 Abs. 4 Buchstabe a und Art. 14 Abs. 5 Buchstabe a DS-GVO).

Wir empfehlen deshalb, das unter 3. genannte **Verarbeitungsverzeichnis** (evtl. ohne Geschäftsgeheimnisse, wenn solche etwa bei den verwendeten sicherheitstechnischen Komponenten schutzwürdig erscheinen) in der Praxis, etwa im Wartezimmer, **gut sichtbar aufzuhängen**. Besonders Interessierten kann eine Kopie ausgehändigt werden.

Die Informationspflicht wird erfüllt, denn:

a) dDas ausgehängte Verarbeitungsverzeichnis kann von interessierten Patienten gelesen werden.
b) Dem Patienten ist ohnehin bekannt, wer mitbehandelnder Leistungserbringer ist; darüber verhält sich die allgemeine Aufklärungspflicht des Arztes nach § 630c BGB.
c) Dem Patienten ist bekannt, dass die Abrechnungsdaten an die KV und seine Krankenkasse bzw. an die HÄVG RZ GmbH gehen.
d) Dem an der HZV eingeschriebenen Patienten ist aus der Einschreibung bekannt, wie der Einschreibungs- und der Abrechnungsweg erfolgt.

5. Speziell für die HZV gilt:

Natürlich muss der Patient, der an der **HZV** teilnehmen will, sich **nach wie vor einschreiben**, also schriftlich zustimmen. Da ändert sich nichts. Aber in die Datenverarbeitung muss er nicht mehr (gesondert) einwilligen. Ist der Patient/Versicherte schon bei seiner Einschreibung in die HZV über den Umfang, den Zweck und den Weg der Verarbeitung seiner Daten und über seine Rechte ordnungsgemäß informiert (das geschieht auch künftig mit dem Aufklärungsbogen (erweiterte Anlage 6.1 zum HZV-Vertragswerk; auf die Anlage 6.2 kann man dann verzichten), erklärt mit seiner Einschreibung "zugleich" (siehe § 295a Abs. 1 Satz 2 SGB V) seine Einwilligung in die Verarbeitung seiner Daten.

Eine neue Anlage 6.1 wird durch die HÄVG AG den Krankenkassen zugeleitet; sie sind verpflichtet, die Verträge entsprechend anzupassen.

6. Abrechnungen für Privatpatienten

Die Einschaltung einer Privatärztlichen Verrechnungsstelle (PVS) bedarf künftig nicht mehr der schriftlichen Einwilligung des Patienten. Denn endlich hat der Gesetzgeber auch insoweit die Organisationshoheit des niedergelassenen Arztes anerkannt. (Die Erforderlichkeit der Einschaltung einer PVS entscheidet allein der Arzt; welche Daten er an die PVS versendet, hängt davon ab, welche Daten die PVS und der Arzt gemeinsam für notwendig halten, um die Abrechnung ordnungsgemäß herzustellen; das häufig und stets fahrlässig angeführte Stichwort "Datensparsamkeit" ist da (wie überhaupt in der ärztlichen Versorgung, die von Genauigkeit, Wissenschaftlichkeit und vollständiger Information lebt) fehl am Platz.

Die PVS wird zwar schon lange als Träger des ärztlichen Berufsgeheimnisses anerkannt (§ 203 Abs. 1 Nr. 7 StGB); neu ist aber, dass der Arzt ihr gegenüber sein Geheimnis eben auch ohne die Einwilligung des betroffenen Patienten befugtermaßen offenbart, § 203 Abs. 3 StGB. Weil das Berufsgeheimnis gesetzlich abschließend im Strafgesetzbuch normiert ist, können die ärztlichen Berufs- und Gebührenordnungen als untergeordnetes Standesrecht daran nichts ändern (etwa § 10 Abs. 6 GOZ).

Manchmal gibt es Durcheinander bei den Datenschützern: Bei der Frage, wer nun neben den Praxisangestellten als "sonstige Person" als befugter Mitwisser des Arztes anerkannt werde, haben einige Autoren ins Feld geführt, die Bundesregierung habe in ihrer amtlichen Begründung zur Neufassung des § 203 StGB (Bundestags-Drucksache 18/11936 Seite 22) ausgeführt: *"Eine Mitwirkung an der beruflichen Tätigkeit ist nur dann gegeben, wenn die mitwirkende Person unmittelbar mit der beruflichen Tätigkeit der schweigepflichtigen Person, ihrer Vorbereitung, Durchführung, Auswertung und Verwaltung befasst ist. Besteht **ein** solcher konkreter Bezug, erscheint die **Einholung einer Einwilligung des Betroffenen*** (also des Patienten, Anm. d. Verf.) ***weiterhin zumutbar und praktikabel**. Unter die mitwirkenden Tätigkeiten fallen [...] Schreibarbeiten, **Rechnungswesen**, Annahme von Telefonanrufen, Aktenarchivierung und -vernichtung, Einrichtung, Betrieb und Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen; Anwendungen und Systeme aller Art, beispielsweise auch von entsprechend ausgestatteten medizinischen Geräten, Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten, Mitwirkung an der Erfüllung von Buchführungs- und steuerrechtlichen Pflichten des Berufsgeheimnisträgers* (also des Arztes, Anm. d. Verf.).

Dieser Text, liest man ihn mit Verstand, ist wegen des Wortes "ein" nicht schlüssig. Deshalb kam der Verfasser schließlich – nach langem Zögern – auf die Idee, es müsse statt "ein" **richtig "kein"** heißen. Seine etwas schüchterne Nachfrage beim Bundesjustizministerium ergab die amtliche Antwort, dass es sich in der Tat um einen **Druckfehler in dem amtlichen Protokoll des Bundestages** handele! (Ein einzigartiger Vorgang, wie der Verfasser ihn noch nie erlebt oder gehört hat.)

Folglich sind alle diese Hilfen (insbesondere für die Anfertigung der Abrechnung!) einsetzbar, ohne dass dazu – wie bisher – die Einwilligung des Patienten eingeholt werden müsste. Das ist eine wichtige Änderung, die mit einer Fülle von Missverständnissen aufräumt.

Der lästigen und situativ häufig unangebrachten gesonderten Einwilligung des Patienten in die Datenverarbeitung durch die PVS bedarf es hier also nicht mehr. Es genügt, dass die Patienten (möglichst nachweisbar, etwa durch gut sichtbaren Aushang des Verarbeitungsverzeichnisses (siehe oben) oder durch ein Merkblatt, das Privatpatienten ausgehändigt wird) wie folgt informiert werden:

- Name und Adresse des für die Datenverarbeitung verantwortlichen Arztes (das ist in der Regel der Behandler bzw. seine Praxis) übermittelt Ihre abrechnungsrelevanten Gesundheitsdaten (den Namen und die Adresse des Patienten und des Rechnungsempfängers; Behandlungsdaten wie Diagnosen, Befunde, Medikationen, erbrachte Leistungen, Krankheitsverläufe) an (Namen und Adresse der PVS) zur Anfertigung und Versendung der Abrechnung an den Patienten bzw. den Rechnungsempfänger.
Die PVS steht unter der gleichen beruflichen Schweigepflicht wie wir.
Bei der PVS erfolgt die Löschung Ihrer Gesundheitsdaten nach vier Jahren. Die Löschung der Adressdaten erfolgt dort nach 10 Jahren; nach vier Jahren werden sie gesperrt.

Die bisher erteilten Einwilligungen sind und bleiben bis auf Weiteres wirksam (Erwägungsgrund 171 Satz 2 zur DS-GVO).

Wir hoffen, Ihnen mit diesen Ratschlägen einen ersten Überblick gegeben zu haben.

Fazit: Es hätte schlimmer kommen können. Das Meiste ist vernünftig; der Umgang mit Patientendaten ist eine Sache absoluter Vertraulichkeit, die zu wahren vom Arzt in der modernen Welt gewisse sinnvolle und notwendige Aufwendungen erfordert.

Dresden, 21. Februar 2018

Dr. Thomas Giesen
Datenschutzbeauftragter der Hausärzteverbände