Die Rechtsabteilung informiert: Datenübermittlungen zwischen Kliniken und Medizinischen Versorgungszentren

Der Hessische Datenschutzbeauftragte hat in seinem jährlich erscheinenden Tätigkeitsbericht u. a. die Frage der Datenübermittlung zwischen einem Medizinischen Versorgungszentrum (MVZ) und einem Krankenhaus beleuchtet. Wir möchten Ihnen im folgenden die relevanten Passagen auszugsweise wiedergeben:

> **4.7.4 Prüfung der Datenübermittlungen zwischen Kliniken und Medizinischen Versorgungszentren**
>
> *Bei der Kommunikation zwischen einer Klinik und einem Medizinischen Versorgungszentrum muss beachtet werden, dass es sich um zwei zu unterscheidende Daten verarbeitende Stellen handelt, die Übermittlung von personenbezogenen Patientendaten auf die jeweils erforderlichen Daten zu beschränken ist und die Einwilligung der Patientinnen und Patienten vorliegen muss. Stichprobenhafte Überprüfungen haben ergeben, dass diese Vorgaben nicht immer eingehalten werden.*
>
> **4.7.4.1**
> **Anlass der Prüfungen**
> Im Gesundheitsbereich gewinnt die strukturierte, interdisziplinäre Zusammenarbeit von Vertragsärztinnen und -ärzten untereinander sowie von Vertragsärztinnen und -ärzten und Angehörigen anderer Heilberufe sowie weiterer Versorgungseinrichtungen zunehmend an Bedeutung. Seit dem Inkrafttreten des Gesundheitsmodernisierungsgesetzes (GMG) am 1. Januar 2004 ist die Gründung eines Medizinischen Versorgungszentrums (MVZ) als eine neue fachübergreifende Versorgungsform möglich. Derartige Zentren sind fachübergreifende ärztlich geleitete Einrichtungen, in denen Ärztinnen und Ärzte als Angestellte oder als Vertragsärztinnen und -ärzte tätig sind. Der Behandlungsvertrag wird zwischen Patientin und Patient (bzw. Krankenkasse) und dem MVZ geschlossen, nicht zwischen Patient und einzelnem im MVZ tätigen Arzt oder Ärztin. Die Vorschriften des SGB V finden entsprechende Anwendung. MVZ haben die gleichen Rechte und Pflichten wie Vertragsärzte im System der gesetzlichen Krankenversicherung. Eigentümer eines MVZ kann eine natürliche oder eine juristische Person sein, z.B. eine Vertragsärztin oder ein Vertragsarzt, eine Apothekerin oder ein Apotheker, eine Klinik oder eine Kapitalgesellschaft. Vielfältige verschiedene Ausgestaltungen und Rechtsformen der MVZ sind möglich (siehe z.B. www.kbv.de). Mitte 2008 gab es bereits ca. 1.100 MVZ bundesweit.
>
> In vielen Fällen wird eine enge Kooperation zwischen MVZ und Klinikum angestrebt. Ziel ist es dabei u.a., dass die Patientin bzw. der Patient gemeinsam umfassend ärztlich betreut wird und sowohl MVZ wie auch Klinik die jeweils erforderlichen Behandlungsdaten rechtzeitig und vollständig zur Verfügung stehen. Dieses Ziel kann auch auf der Grundlage des geltenden Datenschutzrechts realisiert werden. Ebenso wie bei der Kommunikation zwischen Kliniken und Ärztinnen bzw. Ärzten, die als Freiberufler in eigener Praxis tätig sind, muss bei der Kommunikation zwischen Klinik und MVZ jedoch beachtet werden, dass es sich bei dem Klinikum und dem MVZ aus datenschutzrechtlicher Sicht um zwei zu unterscheidende Daten verarbeitende Stellen handelt und die Übermittlung von Patien-

tendaten auf die jeweils erforderlichen Daten beschränkt sein muss und der Einwilligung der Patientinnen und Patienten bedarf.

Zur Klärung der gegenwärtigen Praxis habe ich stichprobenhaft die Kommunikation zwischen MVZ und Krankenhaus geprüft. Da ein MVZ in öffentlich-rechtlicher Rechtsform (d.h. Zuständigkeit des Hessischen Datenschutzbeauftragten) oder auch in privatrechtlicher Rechtsform (d.h. Zuständigkeit des RP Darmstadt, Dezernat Datenschutz) betrieben werden kann, habe ich meine Tätigkeit und die wesentlichen datenschutzrechtlichen Forderungen mit dem RP Darmstadt, Dezernat Datenschutz koordiniert.

4.7.4.2
Prüfungsergebnisse
4.7.4.2.1
Übermittlungsumfang und Rechtsgrundlage
Meine stichprobenhaften Feststellungen ergaben:
Teilweise wird zwischen MVZ und Klinik klar unterschieden. Die Übermittlung von Patientendaten erfolgt im Einzelfall im jeweils erforderlichen Umfang, soweit dies für die Mitbehandlung der anderen Stelle erforderlich ist.
Teilweise waren die Strukturen nicht klar:

- Es erfolgte eine pauschale Übermittlung der Daten von Patientinnen und Patienten des MVZ an das Klinikum, d.h. auch von Personen, die nicht im Klinikum mitbehandelt wurden.
- Umgekehrt bestand die Möglichkeit der Kenntnisnahme der Daten von Patientinnen und Patienten des Klinikums, ohne dass diese (auch) im MVZ behandelt wurden. Im Krankenhausinformationssystem wurden die Ärztinnen bzw. Ärzte des MVZ teilweise als Angehörige des Klinikums, Fachbereich MVZ qualifiziert.

Soweit Daten übermittelt wurden, die zur Mitbehandlung durch die andere Stelle nicht erforderlich waren, war teilweise zuvor eine Einwilligung der Patientin bzw. des Patienten eingeholt worden. Der Wortlaut dieser Einwilligungserklärung bezog sich jedoch auf die Behandlungsdaten, die zur weiteren Mitbehandlung erforderlich sind, und konnte daher keine Rechtsgrundlage sein für die Übermittlung der Daten von Personen, die gar nicht Patientinnen bzw. Patienten der anderen Stelle waren.

Grundsätzlich ist hinsichtlich der Patienteneinwilligung in eine Datenübermittlung noch auf Folgendes hinzuweisen:

Eine **schriftliche** Einwilligung ist für die Übersendung eines Befundes an den Mitbehandler in der Regel nicht zwingend erforderlich. Allerdings kann es von Vorteil für alle Beteiligten sein, wenn die vorgesehenen Datenübermittlungen auf diese Weise klar vereinbart sind. Unabhängig davon kann sich eine Einwilligung stets nur auf den aktuellen Behandlungsfall beziehen, nicht auf sämtliche künftigen Behandlungsfälle im MVZ bzw. in der Klinik. Gemäß § 12 HKHG i.V.m. § 7 Abs. 2 HDSG ist eine **informierte Einwilligung** einzuholen: der oder die Betroffene ist vor der Einwilligung über die Bedeutung der Einwilligung, insbesondere auch über den Verwendungszweck der Daten, aufzuklären. Eine pauschale Ein-

willigung in Datenübermittlungen in allen künftigen Behandlungsfällen erfüllt diese Voraussetzungen nicht.

4.7.4.3
Technischer Ablauf der Datenübermittlungen
Gegenstand der Prüfung war auch der technische Ablauf der Datenübermittlungen: Erfolgt die Übermittlung der Patientendaten per Post, per E-Mail, per Fax oder durch Abruf?

Nach meinen Feststellungen kann zwischen zwei Konstellationen unterschieden werden. Entweder agierte das MVZ autonom wie eine übliche Arztpraxis, oder es kooperierte so eng mit einer Klinik, dass aus dem MVZ auf das Kliniknetz zugegriffen werden konnte.

Im ersten Fall gibt es die üblichen Wege der Übermittlung von Patientendaten. Der Versand per Post ist die Regel, die Übermittlung per Fax erfolgt, wenn es schnell gehen soll, die Kommunikation per E-Mail ist die Ausnahme. Mit den verschiedenen Versandformen verbundene Datensicherheitsprobleme habe ich bei meinen Prüfungen nicht vertieft, da sie nicht spezifisch für ein MVZ waren (zur Kommunikation per Fax s. 20. Tätigkeitsbericht, Ziff. 9.1, zur Kommunikation per E-Mail s. 28. Tätigkeitsbericht, Ziff. 10.1).

Hinsichtlich der Zugriffsmöglichkeiten aus dem MVZ in ein Kliniknetz stellte sich die Situation so dar, dass man sich über eine gesicherte Verbindung vom Arbeitsplatz im MVZ aus, wie von einem klinikinternen Arbeitsplatz, im Klinikinformationssystem (KIS) anmelden konnte. Die vergebene Benutzerkennung war im KIS mit den gewünschten Zugriffsrechten eingerichtet. In diesem Zusammenhang konnten auch Daten vom KIS in die Verwaltungssoftware des MVZ übernommen werden.

Außerdem wurden standardmäßig von der Verwaltungssoftware des MVZ die Stammdaten neuer Patientinnen und Patienten an die Klinik übertragen und dort in das KIS übernommen. Dort wurden sie dann wie Daten neuer Klinikpatientinnen und -patienten behandelt. Die Datenübertragung war technisch ausreichend gegen Zugriffe Dritter abgesichert. Hinsichtlich der eingeräumten Zugriffsrechte ergaben sich aber die oben geschilderten Probleme.

Außer den Datenübermittlungen gab es noch die Zugriffe auf Daten im Zusammenhang mit Fernwartungen. Die Fernwartungen waren nicht in allen Fällen nachvollziehbar. Hierbei handelte es sich ebenfalls um keine MVZ-Problematik, sondern um ein generelles Problem, das seit vielen Jahren den Datenschutz beschäftigt.

„Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (Deutsches Ärzteblatt, A 1026, Heft 19. Mai 2008; www.bundesaerztekammer.de)

10 Fernwartung

Beim Einsatz der Fernwartung müssen grundlegende Sicherheitsvorkehrungen getroffen werden, um der Datensicherheit Genüge zu tun. Bei der Einwahl in die

Fernwartungsaktivitäten muss eine Autorisierung mittels einem aktuell gültigen Passwort erfolgen. Grundsätzlich gilt, dass der Techniker ohne ein gültiges Passwort nicht auf den Praxisrechner zugreifen kann. Nach Beendigung einer Fernwartungssitzung sollte daher eine Änderung des Passwortes erfolgen, somit kann zu einem späteren Zeitpunkt der Techniker nicht ohne Autorisierung auf das System zugreifen.

Die Fernwartungsdaten zwischen dem Computer des Arztes und des Technikers dürfen nur verschlüsselt über eine geschützte Verbindung (s. Kapitel 3.3.2) übermittelt werden. Im Rahmen der Fernwartung sollte darauf geachtet werden, dass die Fernwartung ausdrücklich von der Arztpraxis freigegeben wird. Die Zugriffsrechte des Technikers müssen auf ein Minimum beschränkt werden.

In begründeten Notfällen (z.B. Systemstillstand) kann eine Wartung auf Basis der Echtdaten erfolgen. Grundsätzlich sollten jedoch Testdaten (Testpatienten) dem Fernwartungspersonal zur Verfügung gestellt werden.

Die Fernwartung muss protokolliert werden und vor Ort am Bildschirm durch den Praxisinhaber oder autorisiertes Personal überwacht werden. Weiterhin wird empfohlen, dass der Arzt oder das Praxispersonal Mindestkenntnisse über die Praxis-EDV erwerben, um die Arbeit des Wartungstechnikers qualifiziert begleiten zu können. Anhand des Protokolls sollte jederzeit nachvollzogen werden, welche Veränderungen vorgenommen und auf welche Dateien zugegriffen wurde.

4.7.4.4
Zugriffsausgestaltung innerhalb eines MVZ

Diskutiert wurde bei den Prüfungen auch die Frage, ob **innerhalb eines MVZ** hinsichtlich der Zugriffsberechtigungen der einzelnen Ärztinnen bzw. Ärzte differenziert wird. Nach meinen bisherigen Feststellungen werden in MVZ nur teilweise verschiedene Rollen wie z.B. Administrator, Arzt, Arztgehilfin etc. unterschieden, und Differenzierungen hinsichtlich des Zugriffs durch die Ärztinnen bzw. Ärzte werden vielfach nicht getroffen.

Die verschiedenen Rollen und die damit verbundenen differenzierten Berechtigungen müssen auf jeden Fall eingerichtet werden. Was Differenzierungen hinsichtlich des Zugriffs durch die Ärztinnen bzw. Ärzte anbelangt, so ist zumindest in den Fällen, in denen diese sich nicht wechselseitig vertreten, kein Grund dafür ersichtlich, dass **jeder von ihnen** auf die Daten **aller** Patientinnen und Patienten zugreifen kann. Je höher die Anzahl der Ärztinnen bzw. Ärzte und Fachrichtungen in einem MVZ ist, desto wichtiger wird die Frage nach einer Zugriffsdifferenzierung, d.h. nach einer internen technischen Beschränkung der Zugriffsmöglichkeiten auf die Patientendaten auf den jeweiligen behandelnden Arzt bzw. die Ärztin und die evtl. Vertretung. Dies gilt umso mehr, als nach Information der MVZ rechtlich vorgegeben ist, dass höchstens 30 % der Patientinnen und Patienten fachfremd und höchstens 20 % fachintern von mehr als einer Ärztin oder einem Arzt eines MVZ behandelt werden dürfen.

Teilweise wird von den Patientinnen oder Patienten vor Beginn der Behandlung in einem MVZ eine Einwilligung eingeholt in die Möglichkeit der Kenntnisnahme ihrer Daten durch **alle** Ärztinnen bzw. Ärzte in dem MVZ; teilweise wird dann auch

die Behandlung außer in Notfällen dann abgelehnt, wenn die Patientin oder der Patient die Einwilligungserklärung nicht unterschreibt. Offensichtlich wird hier zumindest erkannt, dass ein Zugriff durch alle Ärztinnen bzw. Ärzte keineswegs selbstverständlich ist. Das Einholen einer Einwilligung in nicht erforderliche Zugriffsmöglichkeiten ist jedoch eine rechtlich problematische und nicht im Interesse der Patientinnen und Patienten liegende Verfahrensweise.

Auch die aktualisierten „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (Deutsches Ärzteblatt, A 1026, Heft 19. Mai 2008; www.bundesaerztekammer.de) sehen in der Technischen Anlage zu diesem Thema Folgendes vor:

> Deutsches Ärzteblatt, A 1026, Heft 19. Mai 2008
>
> 2.4 Mindestmaß der Datenzugriffsmöglichkeiten
>
> Betreffend der Datenzugriffsrechte sollte darauf geachtet werden, dass jeder Benutzer des Computersystems (einschließlich Administrator) ausschließlich Zugriffe bzw. Ausführrechte auf die seinem Tätigkeitsfeld entsprechenden Datenbestände und Programme hat. Insbesondere Programme, welche Verwendung bei der Systemadministration finden, sollten auf die jeweiligen Mitarbeiter beschränkt sein, welche diese für ihre Arbeit benötigen. Die vergebenen Zugriffsrechte sollten in regelmäßigen Abständen auf Aktualität bezüglich der jeweiligen Tätigkeitsfelder überprüft werden.
>
> 2.5 Beschränkung der Arbeit mit Administratorrechten
>
> ... Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Zu diesem Zweck sollten die berechtigten Personen über Zugriffskontrollmechanismen (z.B. Passwörter) legitimiert werden ...

Diese Empfehlungen finden zwar auf MVZ nicht direkt Anwendung. Entsprechende Maßnahmen sind aber im MVZ mindestens ebenso wichtig: Von den Mitte 2008 in Deutschland bereits vorhandenen ca. 1.100 MVZ hatten zu diesem Zeitpunkt einige bis zu 70 Ärztinnen und Ärzte beschäftigt.

Bei unseren Prüfungen wurden wir teilweise darauf hingewiesen, dass nicht jede auf dem Markt erhältliche Arztpraxissoftware die differenzierte Ausgestaltung der Zugriffsrechte und die Benutzerverwaltung so unterstützt, dass die Differenzierungen im Alltag eines MVZ umgesetzt werden können, jedenfalls nicht mit vertretbarem Aufwand. In den o.a. Empfehlungen wird allerdings Folgendes ausgeführt:

> Viele der heute in Arztpraxen eingesetzten Programme verfügen über eine Vielzahl hervorragender Schutzmechanismen. ...

Soweit aufgrund der beschränkten Größe eines MVZ und/oder technischer Probleme eine technische Zugriffsdifferenzierung derzeit nicht in vollem Umfang reali-

siert werden kann bzw. muss, ist zu beachten, dass ein tatsächlicher Zugriff im Einzelfall nur zulässig ist, wenn er erforderlich ist. Es sollte auf jeden Fall ein Zugriff auf die Patientendaten im Streitfall mittels ausreichender Protokollierung nachvollziehbar sein, d.h. schreibende Zugriffe sollten immer nachvollziehbar sein, während lesende Zugriffe jenseits eines Behandlungszusammenhangs protokolliert werden müssen (s.a. Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder, Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme, www.datenschutz.hessen.de/tf007.htm). Als eine Konsequenz müssen alle Nutzenden eigene Benutzerkennungen samt persönlichem Passwort erhalten, damit Protokolleinträge den richtigen Personen zugeordnet werden können. Für evtl. Notfälle können besondere Verfahrensweisen getroffen werden. Eine wesentliche Anforderung betrifft die Dokumentation. Es muss nachträglich möglich sein festzustellen, wer wann welche Zugriffsrechte besessen hat und von wem die Zugriffsrechte vergeben sowie eingetragen wurden. Für die Kontrolle der Protokolle muss ein schriftliches Konzept (Organisationsanweisung o.Ä.) vorliegen, aus dem hervorgeht, wer in welchen Zeitabständen was kontrolliert und welche Maßnahmen bei Anhaltspunkten für einen evtl. Datenschutzverstoß von wem ergriffen werden. Alle Ärztinnen, Ärzte und weitere Beteiligte müssen über die Rechtslage, die Zugriffsprotokollierungen und Protokollauswertungen schriftlich informiert werden.

Zur weiteren Konkretisierung der künftigen Verfahrensweisen sind für das nächste Jahr gemeinsame Besprechungen mit dem RP Darmstadt und der LÄK vorgesehen.

(Auszug aus dem 37. Tätigkeitsbericht 2008 des Hessischen Datenschutzbeauftragten)