Serie: E-Health – Digitalisierung im Gesundheitswesen

Das elektronische Patientendossier (Teil 4):

Zugriffsrechte sollten besser definiert sein

Patientendaten werden in immer mehr Kontexten interessant und relevant. Für deren vernetzte Nutzung braucht es einen Rechtsrahmen. Mit dem Bundesgesetz über das elektronische Patientendossier (ePD) wird dieser für behandlungsrelevante Daten nun geboten. Damit die dabei angestrebten Ziele – Sicherheit, Behandlungsqualität und Effizienz – tatsächlich erreicht werden können, braucht es die breite Akzeptanz des ePD. Diesbezüglich hat der Gesetzgeber nicht alle Stellschrauben richtig justiert. Bis auf Weiteres sind hier die beteiligten Gesundheitsfachpersonen gefordert.

Julian Mausbach

Patientendaten dienen in erster Linie der Behandlung von Patienten und Patientinnen, und sie liegen heutzutage überwiegend elektronisch vor. Die Daten sind allerdings längst mehr als nur Teil der Entscheidungsgrundlage für Behandlungsentscheide. Sie sind in vielen anderen Kontexten relevant. Sie dienen Medizinern etwa als Grundlage für Forschungsprojekte. Patienten nutzen sie zur Selbstvermessung oder zum selbstverwalteten Teilen, das beispielsweise über Plattformen wie midata.coop ermöglicht wird. Der Kernaspekt dieser Nutzung durch Patienten kann mit der Formulierung des deutschen Ethikrats zu Daten im Gesundheitsbereich wie folgt umschrieben werden: Datensouveränität als informationelle Freiheitsgestaltung (1).

«Die Akzeptanz des ePD ist der Schlüssel zu seinem Erfolg. Hierfür hätte hinsichtlich Privacy by Default mehr getan werden können.»

Vielfältige Interessen Dritter

Neben Medizinern und Patienten sind weitere Personen an Patientendaten interessiert. Zu nennen sind hier zunächst (Sozial-)Versicherungen, Industrie und Arbeitgeber. Es ist unschwer erkennbar, dass dieser Kreis noch zu erweitern beziehungsweise auszudifferenzieren ist. Grundsätzlich kann dieser Kreis aber, Einwilligung und/oder Rechtsgrundlage vorausgesetzt, bei der Verfolgung seiner Interessen die Vermutung der Legitimität und Rechtmässigkeit für sich beanspruchen. Personen, die Interessen verfolgen, welche die Grenzen des Rechts überschreiten, können dies nicht. Beispielsweise dann, wenn die Nutzung der Daten Diskriminierung bezweckt oder ein unberechtigter Zugriff auf Daten einen finanziellen Vorteil ermöglichen soll. Mit Blick auf elektronische Patientendaten sind dabei bis heute vor allem Hackerangriffe auf Spitäler und Pflegeheime per Verschlüsselungsviren zu nennen (2, 3).

Dies lässt folgenden Schluss plausibel erscheinen: Sowohl hinsichtlich rechtmässiger Verwendung als auch hinsichtlich des Missbrauchs ist elektronischen Patientendaten ein überragendes und zukünftig wohl noch wachsendes Potenzial zu attestieren (4). Es erscheint daher sinnvoll, den vielfältigen Interessen an ihnen einen Rechtsrahmen gegenüberzustellen, der es gestattet, berechtigte Interessen zu befriedigen, unberechtigte Interessen zu blockieren und Missbrauch zu sanktionieren.

Behandlungsrelevante elektronische Patientendaten sind vorhanden und ziehen vielfältige Interessen auf sich. Ihre vernetzte Nutzung verlangt einen Rechtsrahmen, den das Bundesgesetz über das elektronische Patientendossier (EPDG) für behandlungsrelevante Daten nunmehr bietet.

Als Ziel möglichst viele ePD

Das EPDG ist Teil dieses Rechtsrahmens und daher grundsätzlich zu begrüssen. Seit 15. April 2017 bietet es – mitsamt seinem Verordnungswesen – die Rechtsgrundlage für die vernetzte Nutzung von behandlungsrelevanten Patientendaten durch Gesundheitsfachpersonen und Patienten.

Gerade Spitäler stehen dabei, aufgrund der aus dem EPDG entspringenden Pflicht, sich innert drei Jahren an der Nutzung von ePD zu beteiligen, vor der Aufgabe, die Potenziale für Behandlungsqualität, Sicherheit und Effizienz sicht- und nutzbar zu machen. Dies geht mit beträchtlichen Investitionen, der Überwindung technischer Hürden und weiteren Herausforderungen einher (5). Nicht verwunderlich ist daher der aus den Spitälern vernehmbare Ruf nach Kooperation unter den Leistungserbringern und nach Marketing für das ePD (5). Nachvollziehbar ist auch die Sorge, dass die Bürger das ePD trotz dieser Anstrengungen letztlich dennoch nicht nutzen (5).

Es gilt also sicherzustellen, dass die Bürger das Angebot akzeptieren. Akzeptanz ist dabei deshalb ausschlaggebend, weil die Erreichung der erklärten Ziele – Stärkung der Behandlungsqualität, Verbesserung der Behandlungsprozesse, Erhöhung der Patientensicherheit, Steigerung der Effizienz im

Gesundheitswesen und der Gesundheitskompetenz der Patienten – davon abhängt, dass eine ausreichend grosse Zahl von ePD eröffnet wird. Erst wenn die ePD etabliert sind und durch Gesundheitsfachpersonen und Patienten genutzt werden, können diese Ziele erreicht werden und so die erheblichen Investitionen rechtfertigen.

Zugriffsrechte entscheidend für Akzeptanz

Die breite Akzeptanz des ePD ist der Schlüssel zu seinem Erfolg. Hierfür hätte hinsichtlich Privacy by Default mehr getan werden können.

Ein wesentlicher Aspekt zur Erreichung der benötigten Akzeptanz betrifft die Sicherheit der ePD. Das EPDG selbst sieht umfangreiche Regelungen vor zur technischen und organisatorischen Absicherung der ePD, etwa durch Zertifizierung oder Dokumentierung von Zugriffen. Es ist aber nicht von der Hand zu weisen, dass ein hundertprozentiger Schutz, beispielsweise gegen Cyberattacken, aber auch sonstige unberechtigte Zugriffe letztlich auch hierdurch nicht geschaffen werden kann (6). Ebenso ist zur Kenntnis zu nehmen, dass ebenjene Daten, die über das ePD zugänglich sein werden, sich bereits gegenwärtig zu weiten Teilen in elektronischen Systemen befinden und nicht selten auch elektronisch ausgetauscht werden. Sie sind mithin der Gefahr unberechtigter Zugriffe bereits ausgesetzt (7). Das EPDG führt letztlich nur zu einer weiteren Vernetzung dieser Daten, die Gefahr des unberechtigten Zugriffs an sich begründet es nicht. Dieser Umstand darf nicht dazu verleiten, die Gefahren zu ignorieren oder kleinzureden, sondern muss in der Forderung münden, im Gesundheitswesen insgesamt einen hochstehenden Schutz von Daten einzufordern.

Spezifisch für das ePD folgt daraus zweierlei: Erstens, dass die Gefährdung durch Cyberattacken jedenfalls dann nicht grösser wird, wenn die ePD-Systeme beim Schutz der Daten tatsächlich eine Vorbildfunktion einnehmen. Dies gilt es technisch wie organisatorisch mit den im Gesetz angelegten Mitteln und unter Bezugnahme auf die Besonderheiten der Vernetzung sicherzustellen.

> «Die vorgegebenen Voreinstellungen des EPDG stehen mit dem Datenschutzrecht im Konflikt.»

Zweitens, dass Patienten beim Erstellen eines ePD eine individuelle Abwägung vorzunehmen haben, bei welcher sie die Vorteile der Vernetzung ihrer Daten deren Gefährdung gegenüberstellen. Dies sichert das Gesetz, indem es die Erstellung eines ePD zwingend an die freiwillige und aufgeklärte Einwilligung der Patienten knüpft. Von der dabei zugrunde liegenden Aufklärung verlangt das Gesetz, dass sie eine angemessene Information über die Art und Weise der Datenbearbeitung und deren Auswirkungen umfasst.

Voreinstellungen problematisch

Probleme bereitet dies dann, wenn im Rahmen der Aufklärung die Akzeptanz gegenüber dem ePD schwindet, weil das Gesetz unter dem Aspekt des sogenannten Privacy by Default einiges an Angriffsflächen bietet. So würde man erwarten, dass jene Stellschrauben, die die Bereitschaft zur Eröffnung eines ePD durch den Patienten fördern, in ebendiese Richtung justiert sind. Dies trifft hinsichtlich der Sorge, dass Daten einem zu weiten Kreis von Personen zugänglich sein könnten, aber nicht zu. Zwar sieht das Gesetz die Möglichkeit vor, Daten in verschiedenen Vertraulichkeitsstufen zu klassifizieren und die Zugriffsberechtigung pro Gesundheitsfachperson zu bestimmen. Dies wird aber dadurch entscheidend geschwächt, dass die Voreinstellung der Klassifizierung der Daten so gewählt ist, dass zunächst einmal alle Daten «normal zugänglich» sind. In Kombination mit der Ausgestaltung der Mindestzugangsberechtigung, die sich zwingend auf diese «normal zugänglichen» Daten erstreckt, ergibt sich, dass erst einmal alle zugangsberechtigten Gesundheitsfachpersonen die neu eingestellten Daten einsehen können. Dies auch dann, wenn diese Daten aus Sicht des Patienten sensibel sind. Befunde zu schwerwiegenderen und/oder stigmatisierenden Krankheiten, also sensible Daten, sind aufgrund der Voreinstellung nämlich zunächst «normal zugänglich». Dies wird solange aufrechterhalten, bis der Patient oder subsidiär die Gesundheitsfachperson die Vertraulichkeitsstufe aktiv zu «eingeschränkt zugänglich» oder «geheim» ändert.

Momentan erlaubter Zugriff unverhältnismässig

Die vorgegebenen Voreinstellungen des EPDG stehen mit dem Datenschutzrecht im Konflikt.

Man weiss, dass Datengeber aus Zeitmangel, fehlendem Verständnis, subjektiv empfundener Alternativlosigkeit oder aus gutem Glauben häufig die vorgegebenen Einstellungen von verarbeitenden Anwendungen übernehmen (1) – mithin vermutlich nicht wenige Patienten erst einmal nicht von sich aus die Vertraulichkeitsstufe anpassen. Zudem widerspricht dies dem Verhältnismässigkeitsgrundsatz nach Datenschutzgesetz (8). Dieser besagt unter anderem, dass Personen nur jene Daten bearbeiten dürfen, die zur Erfüllung ihrer Aufgaben benötigt werden. Es ist aber in vielen Fällen so, dass nicht alle beteiligten Gesundheitsfachpersonen alle behandlungsrelevanten Daten für ihre spezifischen Tätigkeiten benötigen.

Diese Voreinstellung mag gewünscht sein, um einen vermeintlich pragmatischen Umgang mit den Dossiers zu fördern. Sie gestattet es, sich als Gesundheitsfachperson bei der ePD-Nutzung ein detailreiches Bild des Patienten zu verschaffen, ohne dass man diesen mit der Bitte um Erteilung erweiterter Zugriffsrechte behelligen muss. Aber dieser Pragmatismus verkennt, dass dies den involvierten Interessen und Sorgen nicht gerecht wird. Mit Blick auf die Akzeptanz zeigt sich das akzentuiert. Die Information, dass sensible Daten weniger sensiblen bis auf Weiteres gleichgestellt sind, erzeugt eher Unbehagen und Zurückhaltung als Vertrauen und Entschlussfreude. Eine Voreinstellung, die unmittelbar klarstellt, dass sensible Daten jedenfalls nur von Personen mit erhöhten Stufen von Zugriffsrechten eingesehen werden können, hätte diese Belastung nicht zu tragen.

Stossend ist, dass der Zugriff auf sensible Daten erst beschränkt ist, wenn der Patient die Daten als «eingeschränkt zugänglich» klassifiziert.

Geltungsdauer unbedingt limitieren

In ähnlicher Weise ist auch die zeitliche Geltungsdauer von Zugriffsrechten zu bemängeln. Das Verordnungswesen zum EPDG verlangt, dass deren Begrenzung aktiv vorzunehmen ist. Immer dann, wenn dies unterbleibt, sind die Zugriffsrechte

Begriffe

Privacy by Default
Privacy by Default heisst «Datenschutz durch datenschutzfreundliche Voreinstellungen» und bedeutet, dass die Werkeinstellungen datenschutzfreundlich auszugestalten sind. Nach dem Grundgedanken sollen insbesondere die Nutzer geschützt werden, die weniger technikaffin sind und zum Beispiel dadurch nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen.

Privacy by Design
Privacy by Design heisst «Datenschutz durch Technikgestaltung» und greift den Grundgedanken auf, dass sich der Datenschutz am besten einhalten lässt, wenn er bereits bei Erarbeitung eines Datenverarbeitungsvorgangs technisch integriert ist.

Quelle: https://www.datenschutzbeauftragter-info.de/

unbefristet gültig. Dies birgt die Gefahr der Einsicht und Bearbeitung von Daten durch Personen, die dies zur Erfüllung ihrer Aufgaben gar nicht mehr benötigen. Im Sinne des Privacy by Design wären hier andere Lösungen zu begrüssen. So könnte für den Fall, dass Zugriffsrechte über einen beträchtlichen Zeitraum hinweg unverändert vorliegen, automatisch eine Benachrichtigung des Systems an die Patienten erfolgen. Dies würde gewährleisten, dass Zugriffsrechte mindestens nicht ohne deren Kenntnis unbefristet fortbestehen.

> «Auch im Notfall können bestimmte Daten sensibel sein. Dies klarstellen zu müssen, überzeugt nicht.»

Im Notfall schaut jeder darauf

Auch im Notfall können bestimmte Daten sensibel sein. Dies klarstellen zu müssen, überzeugt nicht.
Im Bereich des Notfallzugriffs hätte Privacy by Default konsequenter beachtet werden müssen. Das EPDG sieht im Falle eines medizinischen Notfalls vor, dass jede zertifizierte Gesundheitsfachperson in der Schweiz das ePD des Notfallpatienten einsehen kann. Die betreffenden Voreinstellungen gestatten dabei, dass dieser Zugriff auch eingeschränkt zugängliche, also sensible Daten erfasst. Es erschliesst sich auch hier nicht, wieso dem Patienten ein Aktivwerden abverlangt wird, wenn er sensible Daten von diesem Zugriff ausschliessen will. Der Notfallzugriff stellt ohne Zweifel einen grossen Vorteil des ePD dar, der je nach Patient noch dadurch anwachsen kann, dass er sensible Daten umfasst. Dies dem eröffnungswilligen Patienten zu erläutern und ihm zu gestatten, diese Erweiterung zuzulassen, wäre eine Chance für den Eröffnungsprozess. Mit der gewählten Voreinstellung wird diese Chance vertan. Sie ist weniger Ausdruck dessen, dass man die Souveränität über die Daten des Patienten ernst nimmt, als vielmehr ein nächster Ansatzpunkt, zweifelnd von der Eröffnung eines ePD abzusehen.
Im Rahmen der angemessenen Information über die Art und Weise der Datenbearbeitung, als Grundlage für die Einwilligung in die Erstellung eines ePD, sollten diese Aspekte zur Herstellung von Transparenz und Souveränität angesprochen werden. Die Schwächen der Regelung könnte der Patient dann direkt nach seinem Wunsch beheben, was wiederum Akzeptanz gegenüber dem eigenen ePD verspricht. Es ist zu hoffen, dass den Aufklärenden die dafür benötigten Ressourcen zur Verfügung stehen, damit die Schwächen beim Privacy by Default nicht zulasten der Akzeptanz und damit letztlich der Lebensfähigkeit des ePD insgesamt gehen.

Interesse von Dritten im Gesetz nicht berücksichtigt

Das Interesse von Dritten an den Daten wird durch das EPDG nicht abgebildet. Hier wurde eine Chance vertan.
Die vorstehenden Ausführungen verdeutlichen, dass die Akzeptanz des ePD für dessen Bestehen kritisch ist. Wie einleitend angedeutet, sind die Patientendaten längst auch über den Behandlungskontext hinaus relevant. Wenn Patienten tatsächlich in die Lage versetzt werden sollen, die Hoheit und Souveränität über ebendiese Daten auszuüben, sollte dies nicht ausgeblendet bleiben.
Forschungsinteressen, der Aufbau von Registern und sonstige Interessen von Dritten werden im EPDG allerdings nicht abgebildet (9). Das ist insofern nicht verwunderlich, als dies mit der bisherigen Systematik gesetzlicher Regelungen zum Gesundheits- und Medizinrecht in Einklang steht. Diese sieht vor, dass eine Regelung sich entweder auf den Behandlungs- oder den Forschungskontext der medizinischen Tätigkeit bezieht. Was das Forschungsinteresse betrifft, wird das Feld systemgerecht daher ganz dem Humanforschungsgesetz überlassen.
Angesichts der antizipierbaren Relevanz, die Daten in ePD für die Forschung haben, und der umfangreichen Bemühungen, die angesichts dessen unter dem Stichwort «Generalkonsens» getätigt werden, drängt sich die Frage auf, ob nicht dennoch auch im EPDG oder mindestens in der Aufklärung zur Erstellung ein diesbezüglicher Hinweis günstig wäre. Mit den Zielen des EPDG, etwa der Steigerung der Behandlungsqualität oder der Gesundheitskompetenz, schiene dies mindestens nicht zu kollidieren.
Nicht zuletzt hätte dies den Vorteil, dass aufgezeigt wäre, dass Behandlungs- und Forschungskontext immer grössere Schnittmengen aufweisen. Die immer stärkere Verknüpfung dieser Bereiche, wie sie etwa bei der sogenannten «precision medicine» bereits deutlich zutage tritt, wäre für die Gesamtheit der Rechtsunterworfenen durch einen solchen Hinweis sichtbar gemacht. Gerade weil dies auch zu erwartende Aktivitäten rund um das jeweils eigene ePD offenlegen würde, könnte auch dies Akzeptanz schaffen.

Mögliche Verbesserungen

In die Zukunft gedacht, könnte man noch weitergehen. Über die Zertifizierung der Beteiligten, die Zuteilung von elektronischen Identitäten und eine Zugriffsverfolgung sieht das EPDG ein komplexes System vor, das den sicheren Umgang mit Patientendaten gestatten soll. Da wäre es doch sinnvoll, wenn Patienten, die die Nutzung ihrer Daten auch auf andere Kontexte erstrecken wollen, dieses System für den weiteren Gebrauch nutzen könnten. In Kombination mit Schutzmechanismen, die bestimmte Datenverwendungen und Offenle-

gungspflichten ausschliessen, erschiene eine solche Erweiterungsidee bereits weniger provokant. Solche Mechanismen sind dem Recht nicht fremd. So könnten die entsprechenden Regeln zum Versicherungswesen aus dem Gesetz über genetische Untersuchungen beim Menschen einen Ansatzpunkt für deren Gestaltung bieten. Dies ist aber tatsächlich nur im Sinne eines Ausblicks zu verstehen.

Abschliessend gilt es bezüglich der in den Fokus genommenen Aspekte zur Akzeptanz des ePD zweierlei festzuhalten: Erstens ist der Gesetzgeber in die Pflicht zu nehmen, sich der gezeigten Schwächen anzunehmen. Insbesondere Unvereinbarkeiten mit dem Verhältnismässigkeitsgrundsatz sind zu überdenken (8).

Zweitens sind die am ePD beteiligten Gesundheitsfachpersonen dazu aufgerufen, ihre Patienten und Patientinnen bis dahin über die Schwächen zu informieren, sodass diese informiert die Gestaltung ihrer Dossiers vornehmen können.

Solange Privacy by Default nicht gewährleistet ist, ist diese durch Privacy by Infomation sicherzustellen. ▲

Dr. Julian Mausbach
Oberassistent für Straf- und Strafprozessrecht
Universität Zürich
Freiensteinstrasse 5
8032 Zürich
E-Mail: julian.mausbach@rwi.uzh.ch

Es bestehen keine Interessenkonflikte.

Mehr zum Thema Online im Blog des Universitätsspitals Zürich

Begleitend zur Fortbildungsserie «E-Health: Digitalisierung in der Medizin», die in Kooperation mit der Abteilung für Klinische Telemedizin des Universitätsspitals Zürich entsteht, finden Sie im Blog des USZ ergänzende Informationen und Meinungen zum Thema unter: www.blog.usz.ch

Referenzen:
1. Deutscher Ethikrat: Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. (Vorläufige) Stellungnahme, 30. November 2017, 178.
2. NZZ am Sonntag vom 6.2.2017: «Hacker im Spital».
3. Schlingensiepen I: Klinik punktet mit offenem Krisenmanagement. Ärzte Zeitung vom 12.12.2016.
4. Ein Beispiel aus der aktuellen Gesetzgebung ist der erleichterte Zugang zu Patientendaten von verstorbenen Personen durch deren Angehörige, in Art. 16 des revidierten Datenschutzgesetzes.
5. Wittenberg S: Das elektronische Patientendossier (Teil 2): Eine grosse Herausforderung für Spitäler. ARS MEDICI 2017; 107: 988–990.
6. Häni R et al.: Datenschutz und EPD – ein Widerspruch. digma 2017; 17(3): 154–159.
7. Filippi A: Sichere E-Mails und Onlinezugriff für Zahnärztinnen und Zahnärzte. Zahnmedizin Aktuell 2016; 102: 164–165.
8. Widmer B: ePatientendossier und Datenschutz. digma 2017; 17(3): 160–168.
9. Bundesamt für Gesundheit: Erläuterungen zur Verordnung über das elektronische Patientendossier (EPDV). Fassung vom 22. März 2016, 4.

Fachinformationen zum Beitrag von Seite 140/141

Tresiba® Z: Insulin Degludec **I:** Diabetes mellitus Typ 1 bei Erwachsenen, Jugendlichen und Kindern ab 1 Jahr. Diabetes mellitus Typ 2 bei Erwachsenen. **D:** Tresiba® ist ein Basalinsulin zur einmal täglichen subkutanen Verabreichung, möglichst immer zur gleichen Tageszeit. In Fällen, wo eine Dosis vergessen wurde oder wo der übliche Zeitpunkt der Injektion nicht eingehalten werden kann, kann die Dosis zu einem anderen Zeitpunkt verabreicht werden. Ein Minimum von 8 Std. zwischen den Injektionen muss jedoch eingehalten werden. Bei Typ 1 Diabetes mellitus wird Tresiba® gemäss dem individuellen Bedarf des Patienten dosiert. Bei Typ 2 Diabetes mellitus beträgt die empfohlene Anfangsdosis 10 Einheiten pro Tag und kann alleine, in Kombination mit OAD oder mit Bolus-Insulin verabreicht werden. **KI:** Überempfindlichkeit gegenüber dem Wirkstoff oder einem der Hilfsstoffe gemäss Zusammensetzung. **VM:** Beim mit Insulin behandelten Diabetiker besteht grundsätzlich das Risiko leichter oder schwerer Hypoglykämien. Eine nicht ausreichende Dosierung oder Unterbrechung der Behandlung kann bei Patienten, die Insulin benötigen, zu Hyperglykämie führen. **IA:** Der Glukosestoffwechsel wird von einigen Arzneimitteln beeinflusst. Der Insulinbedarf kann vermindert sein durch gleichzeitige Einnahme von oralen Antidiabetika, Alkohol, ACE-Hemmer, β-Blocker, MAO-Hemmer, Salicylaten u.a. Der Insulinbedarf kann erhöht sein durch gleichzeitige Einnahme von Korticosteoride, Danazol, Schilddrüsenhormonen, Sympathomimetika, Diuretika u.a. Bei Anwendung der folgenden Substanzen kann die Insulinwirkung je nach Dosis verstärkt bzw. abgeschwächt werden: Lanreotid, Octreotid-, Salicylsäure-Derivate, Lithium-Salze. UW: Hypoglykämien, Reaktionen an der Injektionsstelle, Lipodystrophie, periphere Ödeme, Urtikaria, allergische Reaktionen. **P:** FlexTouch® 100 E/ml zu 3 ml, FlexTouch® 200 E/ml zu 3 ml, Penfill® 100 E/ml zu 3 ml (B). Ausführliche Angaben finden Sie unter www.swissmedicinfo.ch.

Xultophy® Z: Insulin Degludec 100 Einheiten/ml und Liraglutide 3.6 mg/ml **I:** Xultophy® wird in Kombination mit Metformin oder mit Metformin plus einem Sulfonylharnstoff zur Behandlung des Typ 2 Diabetes mellitus bei Erwachsenen angewendet, wenn Metformin allein, Metformin in Kombination mit einem Sulfonylharnstoff, Metformin in Kombination mit einem GLP-1-Rezeptoragonist oder Metformin in Kombination mit einem Basalinsulin keine adäquate Blutzuckerkontrolle gewährleisten. **D:** Xultophy® ist eine Kombination von Insulin Degludec und Liraglutide zur einmal täglichen subkutanen Verabreichung in einer Injektion, möglichst immer zur gleichen Tageszeit. Bei Hinzugabe von Xultophy® zu OAD beträgt die empfohlene tägliche Anfangsdosis 10 Dosisschritte (10 Einheiten Insulin Degludec/0.36 mg Liraglutide). Xultophy® kann zu einer bereits bestehenden Behandlung mit Metformin oder mit Metformin plus einem Sulfonylharnstoff verabreicht werden. Bei der Umstellung von einem Basalinsulin oder einem GLP-1-Rezeptoragonisten sollten diese vor Beginn einer Xultophy®-Behandlung abgesetzt werden, wobei die empfohlene Anfangsdosis von Xultophy® 16 Dosisschritte (16 Einheiten Insulin Degludec/0.6 mg Liraglutide) beträgt. **KI:** Überempfindlichkeit gegenüber einem oder beiden Wirkstoffen oder einem der Hilfsstoffe gemäss Zusammensetzung. **VM:** Xultophy® sollte nicht bei Patienten mit Typ 1 Diabetes mellitus oder zur Behandlung von diabetischer Ketoazidose angewendet werden. Beim mit Insulin behandelten Diabetiker besteht grundsätzlich das Risiko leichter oder schwerer Hypoglykämien. Eine nicht ausreichende Dosierung und/oder Unterbrechung der antidiabetischen Behandlung kann zu einer Hyperglykämie führen. Patienten mit speziellen kardiovaskulären Risiken sollen mit Vorsicht mit Insulin Degludec behandelt werden. Wird eine Pankreatitis vermutet, sind Xultophy® und andere potenziell in Verdacht stehende Arzneimittel abzusetzen. Eine isolierte Erhöhung der Pankreasenzyme unter der Behandlung mit Xultophy® manifestiert nicht zwingend eine akute Pankreatitis. Patienten, welche mit Xultophy® behandelt werden, sollten auf das Risiko einer Dehydrierung aufgrund von gastrointestinalen Nebenwirkungen hingewiesen werden und Vorsichtsmassnahmen treffen, um eine Austrocknung zu vermeiden. **IA:** Der Glukosestoffwechsel wird von einigen Arzneimitteln beeinflusst. Der Insulinbedarf kann vermindert sein durch gleichzeitige Einnahme von oralen Antidiabetika, ACE-Hemmer, ß-Blocker, MAO-Hemmer, Salicylaten u. a. Der Insulinbedarf kann erhöht sein durch gleichzeitige Einnahme von oralen Kontrazeptiva, Korticosteroide, Danazol, Schilddrüsenhormonen, Sympathomimetika, Diuretika u. a. Bei Anwendung der folgenden Substanzen kann die Insulinwirkung je nach Dosis verstärkt bzw. abgeschwächt werden: Lanreotid, Octreotid-, Salicylsäure-Derivate, Lithium-Salze. **UW:** Hypoglykämien, Appetitverlust, Übelkeit, Durchfall, Erbrechen, Obstipation, Dyspepsie, Gastritis, Bauchschmerzen, Flatulenz, gastroösophaler Reflux, Ruktus, Reaktionen an der Injektionsstelle, Urtikaria, Dehydrierung, Hautausschlag, Pruritus, Hypersensitivität, Erworbene Lipodystrophie, allergische Reaktionen, erhöhte Herzfrequenz. **P:** 3 Fertigpens zu 3 ml, (B). Ausführliche Angaben finden Sie unter www.swissmedicinfo.ch.