Datenschutz – einige Grundsätze für den Praxisalltag

La protection des données – quelques principes pour la pratique quotidienne

URSULA UTTINGER

Patientendossiers sind sensible Daten. Wie mit ihnen in fortschreitender Digitalisierung sicher und korrekt umgegangen werden soll, erläutert die Präsidentin des Datenschutz-Forums Schweiz.

Les dossiers des patients sont des données sensibles. La présidente du Forum de la protection des données Suisse explique comment traiter ces données de manière sûre et correcte dans un contexte de numérisation croissante.

Bereits seit 2014 liest man regelmässig, dass Hacker in die Computer von Spitälern eindringen und Lösegeld verlangen. So sollen im April und Juni 2014 bei einem Cyberangriff auf den amerikanischen Krankenhausbetreiber «Community Health Systems», der um die 200 Spitäler in verschiedenen US-Staaten betreibt, 4,5 Millionen Daten von Patienten in die Hände von Kriminellen gelangt sein [1]. Was mit diesen Daten passierte, ist nicht bekannt.

Ein Cyberangriff kann unangenehme Folgen haben. Im Februar 2016 wurde das «Hollywood Presbyterian Medical Center» nach einer Cyberattacke erpresst: E-Mails funktionierten nicht mehr, Laborbefunde konnten nicht eingesehen werden. Patientendaten wurden so verschlüsselt, dass das Krankenhaus die Daten nicht mehr lesen konnte. Einige Patienten mussten verlegt werden. Schlussendlich bezahlte das Spital 9000 Bitcoins – eine digitale Währung, die absolute Anonymität ermöglicht. 9000 Bitcoins entsprechen in etwa 3,4 Millionen Euro [2]!

Die Cyberangriffe beschränken sich aber keineswegs auf die USA. Auch in Deutschland sind mehrere Fälle bekannt. Unter anderem traf es das Lukas-Krankenhaus bei Düsseldorf. Das Spital konnte vorübergehend nur einfachere Operationen durchführen, kompliziertere Herzoperationen mussten

Des histoires de hackeurs qui pénètrent dans les ordinateurs d'hôpitaux pour ensuite réclamer des rançons paraissent régulièrement depuis 2014. En avril et juin 2014, une cyberattaque visant l'opérateur hospitalier américain «Community Health Systems» qui gère près de 200 hôpitaux dans différents états américains a permis à des criminels de s'emparer des données de 4,5 millions patients [1]. On ignore ce qu'il en est advenu.

Les conséquences d'une cyberattaque peuvent être désagréables. En février 2016, le «Hollywood Presbyterian Me-

© Cifi86 – Fotolia

Cyberangriffe können für medizinische Institutionen gravierend sein: E-Mails funktionieren nicht, Röntgenbefunde können nicht eingesehen werden, Patientendaten sind unlesbar. I Les cyberattaques peuvent avoir des conséquences sérieuses pour les institutions médicales: les boîtes e-mails ne fonctionnent plus, les résultats de laboratoire ne peuvent plus être consultés, les données des patients sont illisibles.

verschoben oder die Patienten dafür in andere Spitäler verlegt werden [3]. Auch in der Schweiz werden Spitäler nicht verschont. Solche Angriffe werden aber meist nicht an die grosse Glocke gehängt, um keine Nachahmer auf den Plan zu rufen [4].

Einfallstore für Hacker

Viele medizinische Apparate sind mit der Informatik verbunden, haben jedoch keinen hohen Sicherheitsstandard, nur schwache Passwörter oder sogar keine. So können Hacker relativ einfach in Spitäler eindringen. Doch nicht nur Spitäler sind betroffen. Die Digitalisierung nimmt überall zu, Daten werden in eine Cloud ausgelagert und Geräte immer mehr vernetzt. So steigen die Risiken. Doch nicht nur die Geräte, sondern auch Webmail-Accounts, die heute weitverbreitet sind, und Daten auf mobilen Geräten sind Einfallstore für Hacker.

Unbestritten ist: Je grösser eine Einrichtung ist, je heiklere Daten und Informationen die Einrichtung hat, die verändert, gesperrt oder gelöscht werden können, umso höher ist das Risiko, angegriffen zu werden. Das Risiko ist bei heiklen Daten auch bei kleineren Unternehmen und Einzelpersonen nicht zu vernachlässigen.

Datensicherheit und Passwörter

Das Datenschutzgesetz verlangt in Art. 7, dass Personendaten durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen [5]. Dies ist einer der Grundsätze, der von jedem Datenbearbeiter einzuhalten ist.

Datensicherheit beginnt damit, dass jede Person ein eigenes Passwort haben sollte. Es kommt immer wieder vor, dass gerade auch im medizinischen Umfeld in einem Team ein gemeinsames Passwort genutzt wird. Damit wird ein Nachweis verunmöglicht, wer zuletzt Daten bearbeitet hat. Bei den heutigen Programmen wird automatisch gespeichert, wann und welcher User etwas geändert hat. Bei gemeinsamen Accounts ist nur der Account ersichtlich, aber nicht der User. Es könnte jede Person sein, die von diesem Account aus gearbeitet hat.

Wichtig ist auch, ein sicheres Passwort zu nutzen.

Idealerweise ist ein Passwort 10–12 Zeichen lang, bestehend aus Gross- und Kleinbuchstaben, Zahlen, Sonderzeichen. Entweder arbeitet man mit einem Passwort-Manager (sehr bekannt und auch sicher ist «KeePass» [6]), oder man merkt sich einen Satz, nimmt die Anfangsbuchstaben und setzt zusätzlich Zahlen und Sonderzeichen:

«Am 12. Februar 2017 habe ich im Internet recherchiert» => «a12.F£7hiiIr»

dical Center» a été victime de chantage suite à une cyberattaque: les e-mails ne fonctionnaient plus et les résultats de laboratoire ne pouvaient plus être consultés. Les données des patients avaient été cryptées et elles étaient illisibles pour l'hôpital. Certains patients ont dû être transférés. L'hôpital avait fini par payer 9000 bitcoins, une monnaie numérique garantissant un anonymat absolu, soit près de 3,4 millions d'euros [2]!

Mais les cyberattaques ne se limitent pas aux États-Unis. Plusieurs cas similaires ont eu lieu en Allemagne, notamment l'hôpital Lukas près de Düsseldorf. Il s'est vu forcé de n'effectuer que des opérations simples, de repousser les opérations du cœur ou de transférer des patients vers d'autres hôpitaux pour être opérés [3]. Les hôpitaux suisses ne sont pas à l'abri. Cependant, ces attaques sont généralement passées sous silence afin de ne pas inciter des imitateurs [4].

Des accès pour les hackeurs

De nombreux appareils médicaux reliés à des réseaux informatiques ne disposent pas d'un standard de sécurité suffisamment élevé. Ils sont protégés par des mots de passe trop simples et certains n'ont même pas de mot de passe, ce qui permet aux hackeurs de pénétrer relativement facilement dans les hôpitaux. Ceux-ci ne sont toutefois pas les seuls concernés. La croissance de la numérisation se poursuit dans tous les domaines, les données sont stockées dans des clouds et les appareils sont toujours plus connectés. Tout cela entraîne une augmentation des risques. En plus des appareils, les comptes webmail, très répandus de nos jours, et les données stockées sur des appareils mobiles constituent aussi des voies d'accès pour les hackeurs.

Il est incontestable que les institutions de grande taille dont les données et informations sensibles peuvent être modifiées, bloquées ou supprimées courent un risque élevé de se faire hacker. Cependant, le risque encouru par les petites entreprises et les particuliers ne doit pas être négligé.

La sécurité des données et les mots de passe

L'art. 7 de la Loi fédérale sur la protection des données exige que les données personnelles soient protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées [5]. Il s'agit d'un principe que toute personne qui traite ce type de données doit observer.

La première étape pour la sécurisation des données est que chaque employé dispose de son propre mot de passe. Il arrive fréquemment, notamment dans le milieu médical, qu'une équipe se partage un seul mot de passe. Il est ainsi impossible de déterminer la dernière personne qui a modifié les données. Les programmes modernes sauvegardent automatiquement l'identité de chaque utilisateur et le moment

Passwörter sollten regelmässig geändert werden. Muss jedoch ein Passwort zu oft gewechselt werden, führt dies dazu, dass Passwörter aufgeschrieben werden – oder einfache Passwörter genutzt werden. Deswegen ist es besser, ein Passwort nicht zu oft wechseln, jedoch spätestens dann, wenn man das Gefühl hat, dass das Passwort gehackt worden ist.

Selbstverständlich sollte ein Bildschirmschoner aktiviert sein – wobei ein Bildschirmschoner alleine nicht genügt. Der Bildschirmschoner sollte auch eine Bildschirmsperre bewirken. Die Sperrzeit ist so zu wählen, dass sie das Arbeiten nicht erschwert. Ein Zugang für Unberechtigte soll jedoch zuverlässig verhindert werden. Verlässt man den Arbeitsplatz, sollte die Bildschirmsperre aktiviert werden.

Daten in der Cloud

Gerade kleinere Unternehmen oder Private haben die meisten Daten in einer Cloud gespeichert und keinen eigenen Server mehr. Hat man einen eigenen Server, stellt sich immer wieder die Frage des Back-Ups: Wo werden Back-Ups aufbewahrt? Und sind alle Daten von den Back-Ups auch wirklich wieder abrufbar?

Diese Aufgabe entfällt mit einer Cloud-Lösung. Bei einer Cloud-Lösung braucht es eine sorgfältige Evaluation des Anbieters. Grundsätzlich gilt: Bei Gratis-Lösungen hat der Anbieter meist auch Interessen an den Daten, der Kunde wird indirekt zu einer Art Produkt. Gerade bei medizinischen Daten muss sichergestellt sein, dass keine unberechtigten Dritten Zugriff haben. Dabei sollten auch die Dienstleistungen des Cloud-Anbieters genau geprüft werden: Wie sieht es aus mit der Verfügbarkeit der Daten? Wie schnell können Daten wiederhergestellt werden? Wo liegt der Server? Gibt es eine «End-to-End-Verschlüsselung» [7]?

Werden Daten Dritten übergeben, hat man einen Teil der Herrschaft über sie verloren. Löscht man die Daten auf seinem Account in der Cloud, so ist keineswegs sichergestellt, dass diese Daten endgültig vernichtet sind. Es ist davon auszugehen, dass der Cloud-Anbieter noch Back-Ups und damit noch irgendwo Kopien der Daten besitzt.

Grundsatz der Verhältnismässigkeit

Ein weiterer wichtiger Datenschutzgrundsatz stellt die Verhältnismässigkeit dar. Es sollten nur solche Daten erhoben und bearbeitet werden, die man auch tatsächlich braucht. Im Zeitalter von Big Data, wo möglichst viele Daten gesammelt und dann nach verschiedensten Bedürfnissen analysiert werden, tönt die Forderung nach Verhältnismässigkeit realitätsfremd. Das Datenschutzgesetz verlangt jedoch in Art. 4 Abs. 2 Verhältnismässigkeit [5]. In den anstehenden Gesetzesrevisionen in der Schweiz und in der EU wird Datensparsamkeit postuliert. Man sollte sich kritisch fragen, warum man be-

© Momius – Fotolia

Bei heiklen Daten ist das Risiko eines Angriffs auch bei kleineren Unternehmen und Einzelpersonen nicht zu vernachlässigen. I Le risque encouru par les petites entreprises et les particuliers en ce qui concerne leurs données sensibles ne doit pas être négligé.

des modifications. Les comptes communs n'indiquent en revanche que le compte. Les modifications peuvent avoir été entrées par toute personne qui a travaillé à partir de celui-ci.

Il est par ailleurs crucial d'utiliser un mot de passe sûr.

Idéalement, un mot de passe est composé de 10 à 12 caractères, comprend des majuscules et des minuscules, des chiffres et des caractères spéciaux. Il est possible de travailler avec un gestionnaire de mots de passe (le «KeePass» est très connu et sûr [6]) ou de mémoriser une phrase, d'en retenir les premières lettres de chaque mot et d'y ajouter des chiffres et des caractères spéciaux:

«Le 12 février 2017, j'ai effectué une recherche sur internet» => «L12f£7jaeursi»

Il faut régulièrement changer les mots de passe. Cela entraîne toutefois la nécessité de les noter ou d'avoir recours à des mots de passe plus simples. C'est pourquoi il est préférable de ne pas changer trop souvent de mot de passe, mais au plus tard lorsque l'on pense qu'il a été piraté.

Même si cela ne suffit pas, il s'agit également d'activer un économiseur d'écran qui verrouille l'écran. Le temps de verrouillage doit être fixé de manière à ne pas gêner le travail, le but étant toutefois de bloquer de manière fiable l'accès aux personnes non autorisées. L'écran doit aussi être verrouillé lorsqu'un employé quitte son poste de travail.

Données stockées dans le cloud

Les petites entreprises et les particuliers sauvegardent justement la plupart de leurs données sur un cloud et ne disposent plus d'un serveur à eux. La question des sauvegardes se

stimmte Daten erhebt und wozu man diese braucht. Vor allem ist jedoch wichtig: Haben nur diejenigen Personen Zugriff zu den Daten, die sie für ihre Tätigkeit wirklich brauchen? Gerade Patientendaten sind besonders schützenswerte Personendaten. Den Zugriff auf einen möglichst kleinen Kreis einzuschränken, dient auch dem Schutz des Datenverantwortlichen. Je weniger Personen auf die Daten zugreifen können, desto kleiner ist das Risiko einer fahrlässigen oder absichtlichen Datenschutzverletzung.

Auskunftsbegehren

Ein Thema, das in der Praxis oft vergessen wird, ist der Umgang mit Auskunftsbegehren. Wird ein Auskunftsbegehren gestellt, müssen sämtliche Daten über die anfragende Person herausgegeben werden [5]. Je mehr Daten vorhanden sind, umso umfangreicher fällt die Herausgabe aus. Zwar werden Auskunftsbegehren gestützt auf Art. 8 des Datenschutzgesetzes (DSG) nicht oft gestellt – mit Ausnahme von gewissen Branchen wie Adresshandel, Wirtschaftsauskunftei, Kundenbindungsprogrammen oder auch Assekuranz –, dennoch muss jeder Inhaber einer Datensammlung wissen, wie mit dem Auskunftsbegehren umzugehen ist.

Inhaber einer Datensammlung ist, wer über den Inhalt und den Zweck einer Datensammlung bestimmt. Bei einer extensiven Auslegung sind bereits zwei Visitenkarten von zwei unterschiedlichen Personen eine Datensammlung. Sicher sind Patientendossiers, elektronisch oder in Papierform, eine Datensammlung. Geht ein Auskunftsbegehren ein, ist die Identität der anfragenden Person zu kontrollieren. Anschliessend sollte in sämtlichen Datensammlungen geprüft werden, ob Daten über diese Person vorhanden sind. Falls ja, stellt sich die Frage, ob allenfalls ein Grund besteht, die Daten zurückbehalten zu können. Dies dürfte in der Physiotherapie selten der Fall sein.

Ein Auskunftsbegehren muss grundsätzlich innert 30 Tagen erfüllt werden [8]. Sämtliche Daten sind in Kopie herauszugeben. Eine Ausnahme stellen persönliche Arbeitshilfsmittel dar. Behandlungsrelevante Daten dürften nicht darunterfallen. Persönliche Notizen sollten im Normalfall in der offiziellen Dokumentation Eingang finden. Es lohnt sich also, bei der Niederschrift und Aufnahme in die Patientendokumentation sorgfältig vorzugehen und abwertende Formulierungen zu vermeiden.

Auch Mitarbeitende haben das Recht, ein Auskunftsbegehren zu stellen. Das bedeutet, dass in einem solchen Fall sämtliche Daten aus dem Personaldossier zu kopieren und herauszugeben sind.

Sobald ein Auskunftsbegehren gestellt wird, dürfen Daten nicht vernichtet werden. Ob tatsächlich sämtliche Daten herausgegeben worden sind, wird in der Praxis kaum überprüfbar sein. Bei einer absichtlich falschen oder unvollständigen

pose régulièrement si l'on dispose d'un serveur particulier: où les stocker? Les données des sauvegardes peuvent-elles d'ailleurs réellement être consultées à nouveau?

Cette tâche devient superflue avec un cloud, une solution qui nécessite toutefois une évaluation minutieuse des fournisseurs. Dans le cas des solutions gratuites, les fournisseurs ont souvent un intérêt pour les données du client qui devient indirectement une sorte de produit. Il faut s'assurer que les tiers non autorisés n'y ont pas accès, particulièrement pour les données médicales. Les prestations de service du fournisseur doivent également être examinées de près: qu'en est-il de la disponibilité des données? à quelle vitesse peuvent-elles être récupérées? où se trouve le serveur? existe-t-il un «chiffrement de bout en bout» [7]?

Transmettre des données à des tiers entraîne une perte de la maîtrise que l'on a sur elles. Supprimer des données sur son compte dans le cloud ne garantit aucunement la suppression définitive de ces données. Il faut partir du principe que le fournisseur de cloud dispose encore quelque part de sauvegardes, donc de copies des données.

Le principe de proportionnalité

La proportionnalité constitue un autre principe important de la protection des données. Seules des données effectivement utilisées devraient être saisies et traitées. À l'ère du big data, où le plus de données possibles sont collectées et analysées pour les besoins les plus différents, une exigence de proportionnalité semble irréaliste. L'article 4 al. 2 de la Loi sur la protection des données en stipule toutefois la nécessité [5]. Des révisions légales à venir en Suisse et dans l'Union européenne postulent le principe d'économie des données. La question critique de savoir pourquoi certaines données sont saisies et quelle utilisation en sera faite devrait être posée. La question la plus importante reste toutefois de savoir si les personnes qui ont effectivement besoin de ces données pour leur activité sont les seules à y avoir accès.

Les données des patients sont des données personnelles particulièrement sensibles. En limiter l'accès à un cercle aussi restreint que possible protège également le responsable des données. Réduire le nombre de personnes qui ont accès aux données permet de diminuer le risque de violation de la protection des données.

Demandes d'accès

Dans la pratique, on oublie souvent la question des demandes d'accès aux données personnelles. Dans ces cas, les données relatives à la personne qui effectue la demande doivent être communiquées [5]. Plus le nombre de données est important, plus la communication sera grande. Tout titulaire d'un recueil de données doit être à même de traiter une de-

Das Datenschutzgesetz verlangt in Art. 7, dass Personendaten gegen unbefugtes Bearbeiten geschützt werden müssen. I L'art. 7 de la Loi sur la protection des données exige que les données personnelles soient protégées contre tout traitement non autorisé.

Auskunft besteht das Risiko einer strafrechtlichen Verurteilung gemäss Art. 34 DSG [5]. Werden also bewusst Daten zurückbehalten, macht man sich strafbar.

Ein korrekter Umgang mit den Daten ist geboten

Mit der fortschreitenden Digitalisierung werden die datenschutzrechtlichen Herausforderungen grösser. Ein korrekter Umgang lohnt sich für den Datenbearbeiter als auch die betroffene Person. Der korrekte Umgang ist immer im konkreten Einzelfall zu prüfen.

Literatur I Bibliographie

1. http://www.spiegel.de/netzwelt/netzpolitik/us-krankenhaeuser-hacker-stehlen-daten-von-4-5-millionen-patienten-a-986804.html – besucht am 12.2.2017.
2. http://www.heute.at/news/welt/Hacker-blockieren-Patientendaten-von-US-Spital;art23661,1259693 – besucht am 12.2.2017.
3. http://www.inside-it.ch/articles/42969 – besucht am 12.2.2017.
4. http://m.20min.ch/schweiz/news/story/14425517 – besucht am 12.2.2017.
5. SR 235.1 Bundesgesetz über den Datenschutz (DSG).
6. Merkblatt Passwort-Manager, Datenschutzbeauftragter Kanton Zürich, April 2016, S. 3.
7. http://www.computerwoche.de/a/acht-tipps-fuer-die-sichere-cloud,2536315 – gelesen am 12.2.2017.
8. Art. 1 Abs. 4 Verordnung zum Bundesgesetz über den Datenschutz (VDSG); SR 235.11.

mande d'accès, bien que les demandes d'accès sur la base de l'art. 8 de la Loi sur la protection de données soient relativement rares, à l'exception de certains secteurs tels que le commerce d'adresses, les renseignements économiques, les programmes de fidélisation de la clientèle ou les assurances.

Est considérée comme titulaire d'un recueil de données, toute personne en mesure de décider du contenu et du but d'un recueil de données. Dans une interprétation extensive, les cartes de visite de deux personnes différentes constituent déjà un recueil de données. Les dossiers des patients, au format électronique ou papier, en sont donc clairement. En cas de demande d'accès, l'identité de la personne à l'origine de la demande doit être contrôlée. Il s'agit ensuite d'examiner le recueil de données en vue de trouver des données sur cette personne. Le cas échéant, la question de la raison pour laquelle ces données peuvent être conservées doit se poser. Cela devrait rarement être le cas en physiothérapie.

Une demande d'accès doit en principe être exécutée sous 30 jours [8]. Toutes les données doivent être transmises sous forme de copies. Les outils de travail personnels constituent une exception. Les données pertinentes pour le traitement ne peuvent en faire partie. Les notes personnelles doivent normalement être incluses dans la documentation officielle. Il vaut donc la peine de procéder avec prudence lors de la transcription et de l'inclusion dans la documentation du patient et d'éviter les formulations péjoratives.

Les collaborateurs ont également le droit de faire une demande d'accès. Cela signifie que, dans un tel cas, l'ensemble des données du dossier personnel doit être copié et communiqué.

Dès qu'une demande d'accès a été déposée, les données ne peuvent plus être supprimées. Il est difficile en pratique de s'assurer que l'ensemble des données a vraiment été communiqué. En cas de renseignements intentionnellement erronés ou incomplets, le fautif court le risque d'une condamnation pénale selon l'art. 34 de la Loi sur la protection des données [5]. Quiconque retient donc volontairement des données se rend punissable.

Un traitement correct des données s'impose

La numérisation croissante augmente également les défis en termes de protection des données. Il vaut la peine de traiter correctement ces documents, tant pour les personnes qui traitent les données que pour celles qui sont concernées. Le traitement adapté doit toujours être examiné au cas par cas.

Ursula Uttinger, lic. iur. / exec. MBA HSG, ist Präsidentin vom Datenschutz-Forum Schweiz und Datenschutzexpertin bei der Integratio GmbH in Zürich.

Ursula Uttinger, lic. en droit/MBA, est la présidente du Forum de protection des données Suisse et experte en protection des données chez Integratio GmbH à Zurich.