Informatik Spektrum
https://doi.org/10.1007/s00287-020-01317-9

FORUM

Digitalisierung im Gesundheitswesen

Ursula Sury[1]

Ausgangslage

Die Welt befindet sich momentan aufgrund der Corona-Pandemie (auch COVID-19 genannt) in einer außerordentlichen Lage. Durch die anhaltende Pandemie haben sich vermehrt Diskussionen betreffend der Digitalisierung der im Gesundheitswesen tätigen Akteure entfacht. Spitäler, Praxen und Therapeuten reichen bei den Kostenträgern unzählige Rechnungen ein. Der Rechnungsversand funktioniert routiniert. Vielfach gehören aber weitere Dokumente zu den Rechnungen, wie bspw. Aufnahmen bildgebender Verfahren, Laborbefunde, Austrittsberichte, Überweisungen und sogar Videos. Die bisherige Trägheit der digitalen Transformation im Gesundheitswesen ist einerseits durch die strengen Auflagen des Gesetzgebers, anderseits durch die datenschutzrechtlichen Sicherheitsbedenken und die Furcht vor der zunehmenden Cyber-Kriminalität zu erklären.

Patientendaten enthalten sehr sensible Informationen, die nicht in unbefugte Hände geraten dürfen. Hier müssen die Akteure im Gesundheitswesen mit entsprechenden Sicherheitsmaßnahmen dafür sorgen, dass die Daten ihrer Patienten bestmöglich gegen allfällige Attacken geschützt sind. Die digitale Transformation im Gesundheitswesen bedingt, dass die Akteure bei solchen anspruchsvollen Digitalisierungsprojekten die datenschutzrechtlichen Auflagen präzise umsetzen.

Digitalisierung im Gesundheitswesen

Bei all den komplexen Anforderungen und Schweiz-spezifischen Herausforderungen ist eines gewiss: Wenn es gelingt, dringende Fragen in Bezug auf die Sicherheit der Daten in den Griff zu bekommen, ist das Potenzial immens. Durch die Digitalisierung entsteht ein elektronischer Informationskreislauf von Aufnahme, Übermittlung, Verarbeitung und Interpretation von Gesundheitsdaten. Arztbriefe, Labordaten, Röntgenbilder, Diagnose- und Medikationslisten stehen in digitalisierter Form zur Verfügung und können jederzeit abgerufen werden. Das schafft Transparenz und beschleunigt Abläufe. Gesundheitsakteure erhalten einen schnelleren Überblick über den Zustand des Patienten und können notwendige Behandlungsschritte schneller einleiten. Davon profitiert nicht zuletzt der Patient. Die engere Vernetzung und Abstimmung der verschiedenen Leistungserbringer vereinfacht die gesamtheitliche Betrachtung der Gesundheit eines Patienten.

Neben den Patienten profitieren auch alle anderen Beteiligten von digitalen Strukturen. So haben beispielsweise Big-Data-Technologien das Potenzial, tiefgreifende Veränderungen in den Behandlungsmethoden zu bewirken. Die bestehenden Datenmengen stellen eine wertvolle Basis dar, um aus ihnen neue wissenschaftliche Erkenntnisse zu ziehen oder in schwierigen und komplexen Angelegenheiten schnelle Entscheidungen zu finden – die richtigen Analysetools vorausgesetzt.

Datenschutz & Digitalisierung im Gesundheitswesen

Laut Schweizer Bundesgesetz über den Datenschutz (DSG) sind Personendaten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Jeder private oder staatliche Akteur, der solche Personendaten speichern, bearbeiten oder weitergeben will, darf dies nur aufgrund einer gesetzlichen Grundlage oder einer Einwilligung der betroffenen Person. Der Eingriff in die Persönlichkeit der betroffenen Person muss nach Art. 4 DSG verhältnismäßig und zweckmäßig sein. Zusätzlich müssen die bearbeiteten Daten richtig und sicher sein gemäß Art. 5 und 7 DSG.

Die Datensicherheit ist nach Art. 7 DSG durch technische und organisatorische Maßnahmen zu gewährleisten. Die Gefahren, die mit Informationssystemen verbunden sind, lassen sich mit technischen und organisatorischen

✉ Ursula Sury
martina.spaqi@dieadvokatur.ch

[1] Luzern, Schweiz

Published online: 06 October 2020

Maßnahmen verringern. So muss ein Informationssystem, das Personendaten enthält, bestimmten Kriterien genügen, um die Sicherheit dieser Daten zu gewährleisten. Technische Maßnahmen hängen direkt mit dem Informationssystem zusammen. Organisatorische Maßnahmen hingegen betreffen das Umfeld des Systems, insbesondere die Personen, die es nutzen. Nur ein Zusammenspiel beider Arten von Maßnahmen verhindert die Vernichtung oder den Verlust von Daten sowie Irrtümer, Fälschungen und den unberechtigten Zugang. Diese Maßnahmen gehören zum Lebenszyklus eines Informationssystems und müssen auf jeder Stufe des Systems greifen.

Welche Fragestellungen müssen konkret bei der Sicherheit beachtet werden? Wo stehen die Datenserver, und wie kann unter Berücksichtigung aller beteiligten Personen deren Sicherheit garantiert werden? Des Weiteren muss festgelegt werden, wie die Daten bspw. eingesehen oder geändert werden können. Dies alles bringt unterschiedliche Sicherheitsanforderungen mit sich: Die Computer der Mitarbeiterinnen und Mitarbeiter dürfen nur für die Personen mit Zugangsberechtigung zugänglich sein. Zudem müssen sie gegen jeglichen Zugriff von außen geschützt werden. Solche Zugriffsversuche können vor Ort stattfinden, indem bspw. eine nicht berechtigte Person den Raum betritt, aber auch von außerhalb der Organisation, indem ein Unberechtigter über das Netz auf das System zugreift. Schließlich muss entschieden werden, welche Spuren des physischen und des elektronischen Zugangs protokolliert werden sollen.

Nach Umsetzung der oben aufgeführten Maßnahmen kann man davon ausgehen, dass der Zugang zu den Daten sowohl physisch als auch in Sachen Bearbeitung sicher ist. Nun geht es darum, diese Sicherheit während des ganzen Lebenszyklus der Daten zu gewährleisten.

Die Daten müssen vom Moment ihrer Einspeisung in das System über alle Bearbeitungsschritte bis hin zu ihrer Vernichtung, Anonymisierung oder Archivierung unversehrt und vertrauenswürdig bleiben. Sie können dabei innerhalb der Organisation von dazu Berechtigten oder aber auch in Drittorganisationen im Auftragsverhältnis bearbeitet werden. Oft werden die Daten im Rahmen ihrer Bearbeitung zudem auf mobile Datenträger wie USB-Sticks, externe Festplatten usw. geladen. Es ist deshalb ratsam, die Bearbeitungen, die vorgenommen werden, zu dokumentieren. Falls Probleme auftauchen, ist dann besser nachvollziehbar, wie sie entstanden sind. Die heutige Kommunikationstechnologie ermöglicht es, rasch und einfach Informationen auszutauschen. Der Datenschutz muss auch bei der Übermittlung sichergestellt werden. Für die Verhinderung von Missbräuchen müssen alle diese Aspekte und Situationen unter die Lupe genommen werden.

Fazit

Die Digitalisierung im Gesundheitswesen ist ein unausweichlicher Prozess. Die Weichen dafür sind durch das Datenschutzgesetz gestellt. Die neuen Kommunikationsmöglichkeiten bieten einen effizienten Datenaustausch zwischen den Akteuren im Gesundheitswesen. Da es sich bei Gesundheitsdaten um besonders schützenswerte Personendaten handelt, müssen die Akteure ihre Pflichten im Datenschutz kennen und umsetzen.