13 ZEILEN KÜRZEN

Datenschutz und Digitalisierung

„Die Schwachstelle ist der Mensch"

Die zunehmende Digitalisierung ist Fluch und Segen zugleich: Digitale Anwendungen verkürzen Wege für Patienten und vereinfachen vielfach den medizinischen Arbeitsalltag. Doch damit Patientendaten reibungslos aufgerufen, getauscht, geteilt und genutzt werden können, braucht es strenge Regeln für den Datenschutz und jede Menge Know-how der GLG-Experten.

„Es ist ein Grundsatz für alle GLG-Mitarbeiterinnen und Mitarbeiter, dass nur die Daten eingesehen und verwendet werden dürfen, die für die Aufgabenerfüllung notwendig sind."

Prof. Dr. Angelika Kreitel
GLG-Datenschutzbeauftragte

Die Daten der Patienten sind ein sehr sensibles und wertvolles Gut. „Deshalb gibt es auch besondere Regeln für die Erhebung, die Verarbeitung und den Umgang mit ihnen", sagt die GLG-Datenschutzbeauftragte Prof. Dr. Angelika Kreitel. Patienten im Krankenhaus müssen einen Behandlungsvertrag unterschreiben, in dem genau erfasst wird, welche Daten erhoben und in welcher Weise weiterverarbeitet werden dürfen. „Dabei ist ganz klar geregelt, ob Diagnosen und Behandlungsmaßnahmen zum Beispiel zwischen Stationen ausgetauscht, für fachgebietsübergreifende Besprechungen (z.B. Konsile, Tumorkonferenzen) bereitgestellt oder etwa an den Hausarzt übermittelt werden dürfen", erklärt die Expertin. Der Patient habe natürlich das Recht, nur bestimmte Formen der Verarbeitung und Weitergabe zu erlauben. „Unsere Erfahrung ist aber, dass die Patienten in der Regel allumfänglich zustimmen", so die Fachfrau. Denn Patienten profitieren vom unsichtbaren Datenverkehr, schließlich können sich die Ärztinnen und Ärzte schnell und unkompliziert austauschen, in sehr viel kürzerer Zeit umfassender über die besten Behandlungsmethoden entscheiden – und der Patient muss seine Akte nicht mehr persönlich zu den am Ablauf Beteiligten bringen. Wird ein Patient in die Notaufnahme eingeliefert und kann vor einer Behandlung nicht mehr in die Datenverwendung einwilligen, wird die entsprechende Vertragsunterzeichnung so schnell wie möglich nachgeholt.

Ähnlich wird in den Arztpraxen verfahren: Hier gibt es anstatt eines Behandlungsvertrages eine Einverständniserklärung zur Erhebung und Übermittlung von Patientendaten, die der Patient unterschreiben muss. Auch dabei besteht, wenn nötig, Gelegenheit, einzelnen Bestandteilen zu widersprechen bzw. die Weitergabe bestimmter Daten zu untersagen.

Wer hat Zugriff auf die Patientendaten?

Angaben zu Stamm- und Behandlungsdaten sind natürlich nicht nur für die unmittelbare Behandlung von Patienten wichtig. Auch für die Abrechnung der Behandlungskosten werden sie zugrunde gelegt. Aber: „Es ist ein Grundsatz für alle GLG-Beschäftigten, dass nur die Daten eingesehen und verwendet werden dürfen, die für die Aufgabenerfüllung notwendig sind", sagt Prof. Dr. Angelika Kreitel. Ein Arzt, der also zum Beispiel im GLG Werner Forßmann Klinikum einen Patienten behandelt hat und nun nur aus persönlichem Interesse wissen will, wie es ihm bei seinem anschließenden Aufenthalt im GLG Martin Gropius Krankenhaus ergangen ist, darf die entsprechenden Daten nicht nutzen. „Zur Unterstützung der Datensicherheit folgt die GLG beim Zugriff auf die Patientendaten einem Rollen- und Berechtigungskonzept", erklärt die Datenschutzbeauftragte. „Dabei erhält jeder Beschäftigte gemäß seiner Rolle, also seiner Arbeitsplatzbeschreibung, die Berechtigung zur Nutzung eines eingeschränkten Bereichs von Daten."

Die menschliche Seite

Trotz eines klar definierten Systems von Zugriffsrechten und Erlaubnistatbeständen für die Verarbeitung – „die Schwachstelle ist und bleibt der Mensch". So hat die Datenschutzbeauftragte immer wieder mit Verstößen gegen die Richtlinien zu tun. Einfach einmal einen Kollegen ins eigene Postfach schauen oder den Computer unbeaufsichtigt lassen, das mutet noch harmlos an, wenngleich es ebenfalls nicht erlaubt ist. Drastischer wird es, wenn das Passwort an einen anderen Kollegen weitergegeben wird, der sich dann über einen fremden Account Zugang zu Daten verschaffen kann. „Das ist nicht nur nicht gestattet, sondern auch strafbar", warnt Prof. Dr. Angelika Kreitel. „Wer Passwörter weitergibt, verhält sich genauso falsch wie derjenige, der diese nutzt." Noch eine andere menschliche Schwäche kommt hier zum Tragen: Neugier. Ob es ein Promi oder die Nachbarin oder ein Kollege ist – die Versuchung, sich über ein fremdes Passwort Zugang zu deren Daten zu verschaffen, kann groß sein. Wer solche gravierenden Verstöße begeht, muss nicht nur mit arbeitsschutzrechtlichen Konsequenzen rechnen, sondern auch mit Bußgeld, das von der Brandenburgischen Datenschutzbehörde auferlegt wird. „Zum Glück ist so ein Verhalten die absolute Seltenheit", sagt Prof. Dr. Angelika Kreitel.

Mehr Sensibilität für Datenschutz

Was kann man aber nun tun, um in einem so großen Unternehmen wie der GLG Millionen von Daten zu schützen? Im Fokus sieht die Datenschutzbeauftragten hier jeden einzelnen Mitarbeiter. Sie sagt: „Gesetzlich ist nicht geregelt, wie oft Mitarbeiter geschult werden sollten. Aber eine datensichere GLG sollte in unser aller Sinne sein, deshalb werden alle Beschäftigten in den Krankenhäusern, der Verwaltung und den vielen zugehörigen Einrichtungen regelmäßig geschult." Sehr erfreulich sei, dass die Schulungen gern besucht würden und die Mitarbeiterinnen und Mitarbeiter ohnehin sehr aufmerksam im Umgang mit Patientendaten geworden sind.

Investition in Kommunikationssystem

Wichtigste Helfer bei der Bewahrung des Datenschutzes sind technische Komponenten (siehe Infokasten unten). So verfügt die im Krankenhaus genutzte Software zum Beispiel über einen „Versiegelungsmechanismus", bei dem die Daten von prominenten Patienten oder Mitarbeitern so geschützt sind, dass sie nur vom behandelnden Arzt mit einer Sonderberechtigung geöffnet werden dürfen. Viel häufiger aber als diese Fälle sind Verstöße, die im Alltag fast untergehen: Ein Krankenhaus ist auch ein Kommunikationsbetrieb, hier werden gern schnelle Kommunikationsmedien, Apps, die sich auf jedem Smartphone befinden, genutzt. Das Problem besteht darin, dass diese Daten in den meisten Fällen direkt ins Ausland fließen. Prof. Dr. Angelika Kreitel kündigt deshalb an: „Wir planen die Anschaffung eines betrieblichen Kommunikationssystems, das auf privaten Handys aufgespielt werden kann und mit dem sich die Mitarbeiterinnen und Mitarbeiter ebenso schnell und flexibel austauschen können wie mit WhatsApp – aber eben sicherer."

Unsichtbarer Schutz im Hintergrund

GLG-Beschäftigte kennen es: Eine Mitteilung aus der Abteilung für Informationstechnik (IT) mit Hinweis auf eine verdächtige E-Mail landet im Posteingang. Ist der Absender bekannt und wird die Mail erwartet, machen die Kollegen von der IT mit einem Klick den Weg frei. Wenn nicht, dann ist womöglich ein Angriff von außen vereitelt worden. Kein Einzelfall – Tausende von E-Mails dieser Art sind unterwegs.

„Von den 5.000 bis 10.000 Mails, die täglich in den E-Mail-Postfächern des GLG-Verbunds auftauchen, werden etwa 95 Prozent (!) aussortiert. Die Mehrheit ist Spam, also Datenmüll, z.B. Werbung. Im Rest verbergen sich durchaus gezielte Angriffsversuche", erklärt Frank Kosanke aus der IT-Abteilung. Zusammen mit seinen Kollegen hat er einen Blick darauf, was da so alles seinen Weg ins GLG-Netzwerk sucht. Zum Glück helfen ihnen spezielle Programme dabei, den Großteil der unerwünschten E-Mails abzufangen. Immer wieder müssen die versierten Techniker auch selbst eingreifen, zum Beispiel bei der Freigabe von versehentlich zurückgehaltenen E-Mails. Auch sonst haben die Profis viel zu tun: Alles muss immer auf dem neuesten Stand gehalten und gegebenenfalls angepasst werden. Dazu kommt mit Hilfe der Kollegen der Medizintechnik die Zusammenarbeit mit den Geräteherstellern, die mit dem Einzug von immer mehr digitalen Anwendungen und dem vermehrten Fokus auf Künstliche Intelligenz immer komplexere Systeme anbieten.

Ziel des unsichtbaren Datenschutzes durch die IT ist es, Cyber-Angriffe, die den Betrieb in den Krankenhäusern maßgeblich einschränken oder einen Großteil der GLG technisch lahmlegen könnten, zu vermeiden. Warnende Beispiel gibt es genug – wie etwa das der Angermünder Stadtverwaltung, die durch einen Hackerangriff monatelang nicht richtig arbeiten konnte. Und deshalb wünschen sich Frank Kosanke und seine Kollegen von allen Beschäftigten höchste Aufmerksamkeit und Sorgfalt bei der Unternehmenskommunikation. „Wir wissen, dass es inzwischen nicht mehr die Frage ist, *ob* ein Datenangriff größeren Stils bevorsteht, sondern nur *wann* er eintreten wird", so Frank Kosanke. „Darauf wollen wir vorbereitet sein und setzen deshalb alles daran, gemeinsam mit allen Kolleginen und Kollegen so gut und eng wie möglich beim Datenschutz zusammenzuarbeiten."