Urs Baumberger im Interview mit QUMEA: neues Ungemach im Vormarsch

Cyber Security und Datenschutz fordern Spitaldirektoren

Anfangs Juni fielen die Londoner Spitäler einer Cyberattacke zum Opfer: 800 Operationen mussten verschoben werden, 97 Krebsbehandlungen und 18 gespendete Organe wurden in andere Einrichtungen umgeleitet, so NHS in einer Mitteilung. Schweizer Spitälern können ähnliche Szenarien drohen – ein aufreibendes Thema mit höchster Priorität.

Herr Baumberger – Sie sind als langjähriger erfolgreicher Direktor in der Beratung tätig oder direkt an der Führungsfront ad Interim im Einsatz in den unterschiedlichsten Spitälern der Schweiz. Spitaldirektoren stehen derzeit besonders unter Druck – worauf müssen sie sich und ihre Institution vorbereiten, um für die Zukunft gewappnet zu sein?

Urs Baumberger: Genau, die Herausforderungen in der Gesundheitsbranche sind enorm und entwickeln sich ständig weiter. Neben den bereits bekannten Problemen kommen mit der fortschreitenden Digitalisierung neue Baustellen hinzu, insbesondere im Bereich Datenschutz und Cyber Security. Diese Themen sind nicht neu, gewinnen jedoch an Bedeutung und Dringlichkeit durch sich ständig weiterentwickelnde Technologien. Datenschutz ist entscheidend für das Vertrauen zwischen Ärzten, Spitälern und Patienten, aber auch für den operativen Alltag der Spitäler. Daher müssen Massnahmen ergriffen werden, um Institutionen auf bestehende und zukünftige Herausforderungen in diesem Bereich vorzubereiten.

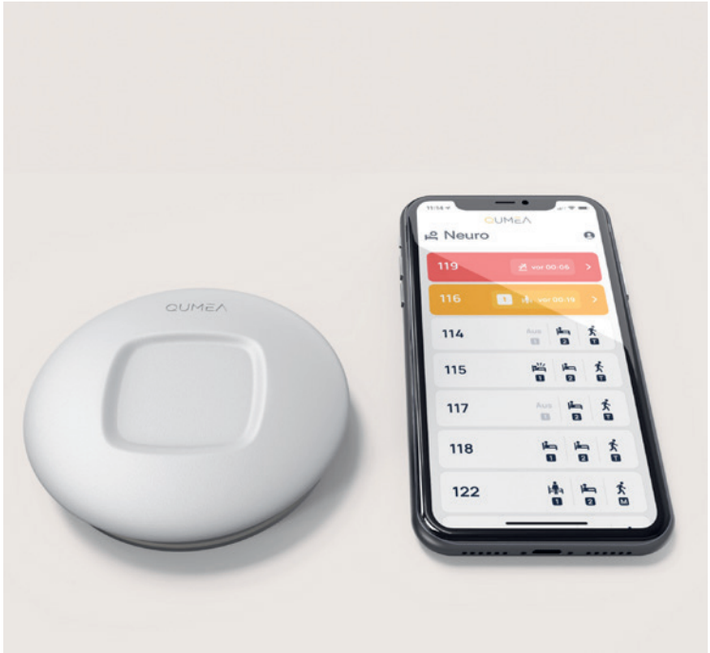
Es braucht eine starke Kultur der Datensicherheit

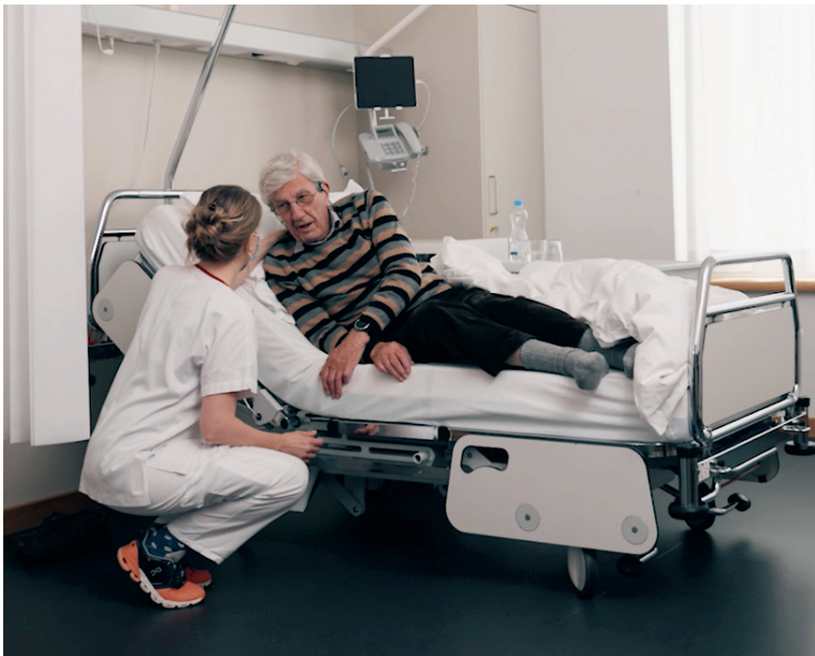
Eine starke Kultur der Datensicherheit innerhalb der Organisation ist wichtig. Alle Mitarbeitenden müssen ihre Rolle im Schutz der Patientendaten verstehen, nicht nur die Schnittstellen mit Patientenkontakt. Vor der Verarbeitung personenbezogener Daten muss die Einwilligung der Patienten eingeholt werden, wobei sicherzustellen ist, dass diese freiwillig und ausreichend informiert erfolgt. Dies erfordert eine gut organisierte Prozessgestaltung entlang des Patientenpfades und muss koordiniert geschehen.

Ein Verarbeitungsverzeichnis, das alle verarbeiteten personenbezogenen Daten, den Zweck der Verarbeitung und die rechtliche Grundlage enthält, ist notwendig und dienlich. Dabei ist das Prinzip der Datensparsamkeit zu berücksichtigen. Dieses besagt, dass nur für die Behandlung relevante personenbezogene Daten erhoben, verwendet und gespeichert werden dürfen. Die Einhaltung dieser Vorgabe ist gesetzlich vorgeschrieben.

Es ist also entscheidend, proaktive Strategien zu entwickeln und durch die Direktion zu forcieren, um den sich ändernden Anforderungen immer einen Schritt voraus zu sein. Dies erfordert kontinuierliche Investitionen in Technologie und Ausbildung, um sicherzustellen, dass Einrichtungen und Personal auf dem neuesten Stand sind. Sichere Passwörter und regelmässige Software-Updates sollten als Standard gelten, werden von Nutzern jedoch nicht selten vernachlässigt. Ebenso wie Backups, die einen kompletten Datenverlust vermeiden können; sie funktionieren nur, wenn sie konsequent

Datensicherheit steht zuoberst: Da Radardaten von Patientenbewegungen keinen Rückschluss auf personenbezogene Informationen zulassen, ist das Monitoring 100 % anonym. Es ist daher unmöglich, auf Patienteninformationen zu schliessen.





durchgeführt werden. Beachtung finden zudem externe Dienstleister, die auf die Einhaltung der Datenschutzvorschriften geprüft und mit denen entsprechende Verträge abgeschlossen werden müssen.

Sich professionell wappnen

Die Sachlage um Cyber Security und Datenschutz ist komplex und für Personen, die keine Spezialisten auf dem Gebiet sind, oft intransparent. Was raten Sie einer Spitalleitung in Bezug auf dieses Thema?

Cyber Security und Datenschutz sind in der Tat ein breites Feld, und eine sorgfältige Herangehensweise ist unerlässlich. Zunächst muss die Spitalleitung sowie das gesamte Personal ein Bewusstsein für die möglichen Konsequenzen eines Sicherheitslecks entwickeln. Der Schutz der Institution geht über die Schulung im richtigen Umgang mit Computern hinaus. Er umfasst auch die sichere Anbindung nach aussen, an Schnittstellen und zu externen Dienstleistern sowie die Sicherung sensibler Daten.

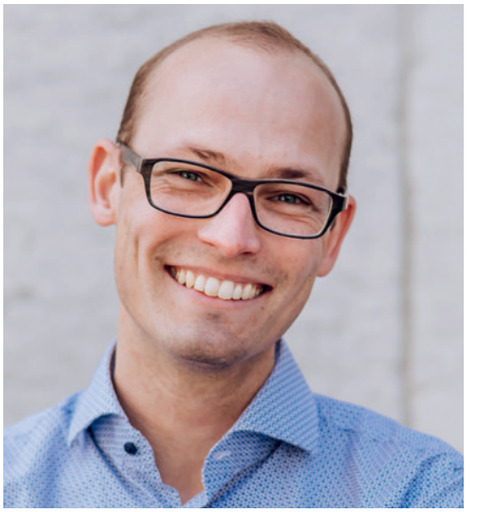
Regelmässige Risikoanalysen sind Aufgabe der Geschäftsleitung und entscheidend, um potenzielle Schwachstellen frühzeitig zu identifizieren und zu beheben. Dies schliesst die Nutzung starker Passwörter, einer Zwei-Faktoren-Authentifizierung und die Implementierung einer End-to End-Datenverschlüsselung ein. Obwohl die Vorstellung eines komplett unhackbareren Spitals unrealistisch ist, sind vernünftige und effektive Massnahmen angezeigt, um sich so gut wie möglich zu schützen und auf den «Worst Case» vorbereitet zu sein.

Die kontinuierliche Überprüfung externer Dienstleister, die Verwaltung von Zugriffsrechten und das Erstellen von Notfallplänen tragen zur Sicherheit bei. Ebenso der Einsatz von Systemen, die Missbrauch verhindern oder zumindest minimieren. Es bedarf kontinuierlicher Anstrengungen und entsprechende Prozesse, um den Anforderungen von Datenschutz und Cybersicherheit gerecht zu werden.

Stichwort «Worst Case»: Wie könnte ein solcher für ein Spital aussehen?

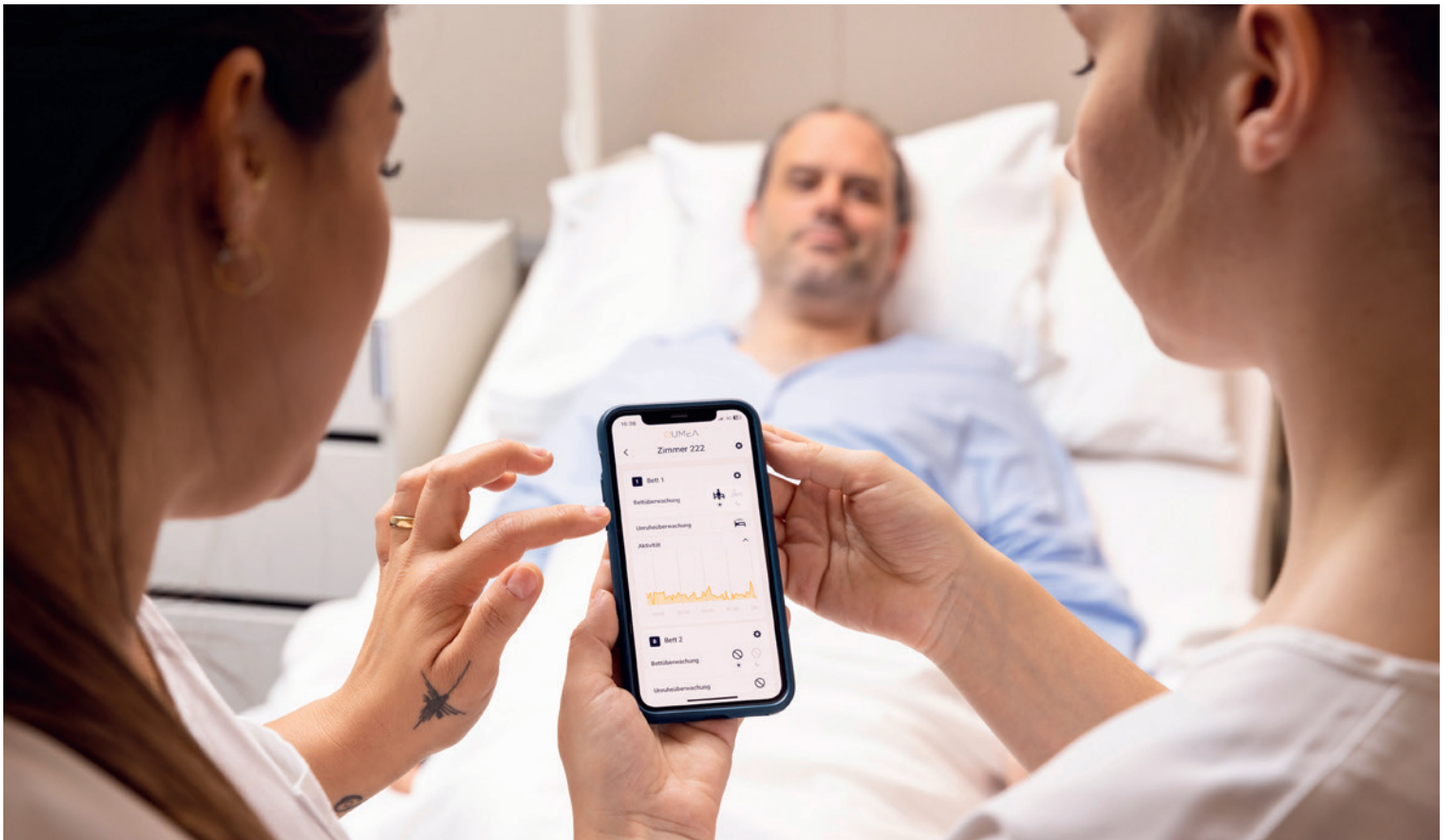
Eine Cyberattacke kann vielfältig ausfallen, ein Worst Case könnte sein: Ein Hacker erlangt Zugriff auf die Patientendatenbank, was zu Einsicht in die Patientengeschichte, Identitätsdiebstahl, Verletzung der Privatsphäre und falschen medizinischen Behandlungen führt. Die Angreifer übernehmen medizinische Geräte, die mit dem Internet verbunden sind, z.B. Herzmonitore, Infusionspumpen oder Beatmungsgeräte, wodurch für Patienten lebensbedrohliche Situationen entstehen.

Ein weiteres Szenario trat jüngst in den Londoner Spitälern ein: Der Ransomware-Angriff infizierte das Krankenhausnetzwerk und blockierte den Zugriff auf kritische Systeme, was Betriebsunterbrechungen, verzögerte Behandlungen und finanzielle Verluste zur Folge hatte.



«Das Mobilitäts-Monitoring von QUMEA basiert auf einem intelligenten 3D Radar. Anders etwa als bei optischen Systemen ist es nicht möglich, aufgrund der Radardaten Rückschlüsse auf individuelle Personen zu ziehen. Die Anonymität wird bereits an der Quelle gewährleistet, was eine präventive Umsetzung von Cyber Security darstellt. So wird nicht nur der Datenschutz konsequent umgesetzt, sondern auch das Vertrauen der Patienten und Mitarbeitenden gestärkt.»
Jonas Reber, CTO QUMEA

Ebenso desaströs ist die Manipulation medizinischer Aufzeichnungen oder Befunde durch einen Hacker, was falsche Diagnosen und Behandlungen zur Folge hat. Oder ein Angriff auf die Kommunikationssysteme des Spitals, der dazu führt, dass Ärzte, Pflegepersonal und Admi-



nistratoren nicht effektiv miteinander kommunizieren können. Weiter kann ein Sicherheitsleck den Verlust oder Diebstahl wichtiger Forschungsdaten verursachen. Und natürlich kann ein Spital auch einen enormen Reputationsschaden erleiden.

Letztlich geht es darum, es gar nicht erst so weit kommen zu lassen; Prävention ist hier der Schlüssel. Durch die Einrichtung starker Verteidigungslinien und die Aufrechterhaltung einer hohen Wachsamkeit kann man viele Risiken minimieren, bevor sie zu einem ernsthaften Problem werden.

Grösstmögliche Sicherheit und Wahrung der Privatsphäre

Im Datenschutz gilt der Grundsatz der Datenminimierung. Wie trägt dieser zur Cybersecurity bei?

Das Erfassen und Nutzen personenbezogener Daten ist auf das notwendige Minimum zu beschränken. Dadurch wird einerseits die Privatsphäre bewahrt, andererseits die individuelle Identität geschützt, da Rückschlüsse auf einzelne Personen gar nicht oder nur schwer gezogen werden können. Damit ist man nicht nur konform mit den gesetzlichen Anforderungen, wie dem eidgenössischen und den kantonalen Datenschutzgesetzen, die verlangen, dass wir verhältnismässig agieren. Wir reduzieren gleichzeitig das Risiko eines potentiellen Datenlecks beträchtlich.

Ein Beispiel, das ich in Bezug auf Datensparsamkeit als besonders vorbildlich sehe, ist das radarbasierte Mobilitäts-Monitoring von QUMEA. Dieses System basiert auf einem 3D-Radarsensor im Patientenzimmer und generiert keinerlei personenbezogene Daten. Diese anonymen Daten genügen dem System, um die Patientenbewegung zu messen und kritische Patientenzustände zu erkennen, um einen entsprechenden Alarm auszulösen und die Pflege rechtzeitig zu informieren. QUMEA ist damit ein hervorragendes Beispiel für Datenminimierung: Für die Erfüllung dieser Aufgabe sind persönliche Merkmale wie Geschlecht, Alter, etc., irrelevant und werden gar nicht erst gesammelt. So wird Missbrauch effizient vermieden und schafft gleichzeitig Vertrauen bei den Patienten und im Team. Das ist ganz anders etwa beim Einsatz einer kamerabasierten Lösung, die ein Bild oder ein Video aufnimmt, auf welche Hacker potenziell zugreifen können.

QUMEA setzt auf Sicherheit

QUMEA ist führend im intelligenten und nahtlosen Mobilitäts-Monitoring im Patientenzimmer. Die eingesetzte Radartechnologie misst kontaktlos und hochsensitiv menschliche Bewegungen. Diese geben Aufschluss darüber, wie sich eine Person bewegt oder in welchem Zustand sie sich befindet. Sturz- oder Dekubitus-Risiken können so früh erkannt und eliminiert werden.

Da Radardaten keinen Rückschluss auf personenbezogene Informationen zulassen, ist das Monitoring 100 % anonym. Im Fall eines Datenlecks ist es unmöglich, aus den Radardaten auf Patienteninformationen zu schliessen. Damit ist der Datenschutz gewährleistet und die Privatsphäre geschützt.

Weitere Informationen

www.qumea.com