FMH SERVICES

Datenschutz ernst nehmen und Vertrauen schaffen

Die Digitalisierung schreitet auch im Gesundheitswesen unaufhaltsam voran und dies mit allen Vor- und Nachteilen. Abläufe können effizienter gestaltet und somit beschleunigt werden. Digitale Hilfsmittel sind auch in Spitälern und Arztpraxen kaum noch wegzudenken. Doch mit der zunehmenden Digitalisierung vergrössert sich auch die potenzielle Angriffsfläche. Da die Konsequenzen von Datenverlust und -manipulation besonders im Gesundheitsbereich gravierend sein können, sind Sicherheitsmassnahmen auf allen Ebenen erforderlich.

Daten über die Gesundheit von Personen gehören zu den «besonders schützenswerten Personendaten» und verlangen dementsprechend einen sehr guten Schutz. Dabei gilt es, solche Daten vor unbefugten Veränderungen, Zerstörung und Missbrauch zu schützen. Falsche oder nicht verfügbare Informationen können gravierende Konsequenzen haben und die Gesundheit, im schlimmsten Fall sogar Leben gefährden[1].

Sicherheitsmassnahmen auf allen Ebenen: Verhalten, Technik und Organisation

Erst mit einem integralen Ansatz für den Schutz sensibler Gesundheitsdaten kann ein möglichst umfassender Schutz erzielt werden. Dieser Ansatz sieht vor, dass dem Thema auf verschiedenen Ebenen Rechnung getragen wird. Sicherheitsmassnahmen lassen sich dabei in drei Kategorien einteilen: verhaltensbezogen, organisatorisch und technisch.

Zu den verhaltensbezogenen Massnahmen gehört beispielsweise die Verwendung von langen komplexen Passwörtern. Damit diese nicht auswendig gelernt werden müssen, empfiehlt sich die Verwendung eines Passwort-Safes. Mit einem solchen Programm können Passwörter einfach gespeichert und sicher aufbewahrt werden. Einen zusätzlichen Schutz bietet der Einsatz der Zwei-Faktor-Authentisierung, wobei sich der Anwender neben dem Passwort mit einem zweiten Faktor anmelden muss. Mögliche zweite Faktoren bieten beispielsweise Authentisierungs-Apps (wie die HIN Authenticator

App) oder eine hinterlegte Identitätsdatei, wie dies beispielsweise im HIN Client der Fall ist. Für den Fall, dass ein Passwort durch unbefugte Dritte gehackt wird, bleibt ihnen der Zugang auf das betreffende Konto verwehrt, da ihnen der zweite Faktor fehlt. Neben dem Schutz von persönlichen Konten ist es wichtig, sensible Daten immer verschlüsselt zu übermitteln (beispielsweise mit HIN Mail). Unverschlüsselte E-Mails bringen erhebliche Gefahren mit sich, da der Inhalt der Nachricht von unbefugten Dritten abgefangen und eingesehen werden können. Die Vertraulichkeit einer unverschlüsselten E-Mail wird folglich oft mit jener einer Postkarte verglichen.

Zu den wichtigsten technischen Massnahmen gehört unter anderem, dass alle IT-Systeme immer auf dem neusten Stand gehalten werden. Mithilfe von regelmässigen und sicher aufbewahrten Backups können im Falle eines erfolgreichen Cyberangriffes verlorene Daten wieder hergestellt werden. Die Wichtigkeit regelmässiger Backups hat sich beispielsweise gezeigt, als die Hirslanden-Gruppe im Herbst 2020 Opfer eines Verschlüsslungstrojaners wurde[2]. Die verschlüsselten Daten konnten dank einem Backup wieder hergestellt werden und die Patientenversorgung war zu keinem Zeitpunkt gefährdet.

Auch organisatorische Massnahmen können dabei helfen, den Schutz sensibler Daten massiv zu erhöhen. Durch sicherheitsrelevante Vorgaben und kontrollierte Abläufe können Risiken minimiert werden. Dazu gehört beispielsweise die Bestimmung von Verantwortlichkeiten oder das Einschränken von Berechtigungen. Vorgesetzte, die mit gutem Beispiel vorangehen, können Mitarbeitende motivieren, das Thema Datenschutz ernst zu nehmen. Ergänzt durch eine regelmässige Schulung der Mitarbeitenden zum Thema Datenschutz und IT-Sicherheit entsteht eine erhöhte Sensibilisierung, welche sich langfristig positiv auf das Verhalten im Umgang mit sensiblen Daten auswirkt.

Durch gezielte Schulung das Bewusstsein für Gefahren schärfen

Für den Schutz von sensiblen Daten sind technische Massnahmen wichtig, doch ein ebenso wichtiger Faktor ist das menschliche Verhalten. Wer sich den Gefahren der Cyberkriminalität bewusst ist, kann diesen mit mehr Sicherheit begegnen und unter Umständen sogar dort eingreifen, wo die Technik versagt. Um Mitarbeitende für das Thema Datensicherheit zu sensibilisieren, empfiehlt sich eine regelmässige und gezielte Schulung. Im Fokus soll dabei nicht die reine Informationsvermittlung stehen, sondern die Schaffung eines langfristigen Bewusstseins für mögliche Gefahren. Eine Datenschutz-Schulung legt eine solide Basis dafür, dass sich jede und jeder ihrer oder seiner Verantwortung bewusst ist und diese im Arbeitsalltag wahrnimmt.

Auch das Bundesamt für Justiz (BJ) weist in seinem erläuternden Bericht zum neuen Datenschutzgesetz (nDSG) ausdrücklich auf die Relevanz von Schulungen und Beratungen hin[3]. Denn aus Sicht des Bundesrates hängen die Umsetzung und Wirksamkeit der Datensicherheit insbesondere auch davon ab, ob die involvierten Personen vorgesehene Massnahmen in Bezug auf IT-Sicherheit und Datenschutz korrekt anwenden. So können durch Schulungen und Beratungen die Risiken von Datensicherheitsverletzungen minimiert werden, beispielsweise durch den bewussten Umgang mit potenziell gefährlichen E-Mail-Anhängen oder Links.

Datenschutz ernst nehmen und Vertrauen schaffen

Patienten und Patientinnen dürfen von ihren Behandelnden eine sorgfältige Behandlung erwarten und somit ein rechtmässiges Verhalten bezüglich des Umgangs mit Patientendaten. Gesundheitsfachpersonen sind verpflichtet, das Patientengeheimnis zu wahren und sie unterstehen dem Datenschutzgesetz. Eine qualitativ hochwertige Behandlung der Patienten bedingt somit unter anderem, dass dem Datenschutz jederzeit Rechnung getragen wird. Ärzte und Ärztinnen, die ihre Verantwortung für den Datenschutz wahrnehmen und dies ihren Patienten gegenüber transparent machen (beispielsweise mit dem HIN Label), tragen dazu bei, das Vertrauensband zwischen Arzt und Patienten zu stärken.

Quellenverzeichnis

1. Nationales Zentrum für Cybersicherheit NCSC, Halbjahresbericht 2020/2, 11.05.2021, https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2020-2.html

2. Neue Zürcher Zeitung, «Cyberangriff auf die Hirslanden-Gruppe: Die Spitäler sind wegen der Pandemie besonders anfällig für Erpressungen», 25.11.2020, https://www.nzz.ch/schweiz/cyberangriff-auf-die-hirslanden-gruppe-die-spitaeler-sind-wegen-der-pandemie-besonders-anfaellig-fuer-erpressungen-ld.1587386

3. Bundesamt für Justiz (BJ), «Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz», Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, 23.06.2021, https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.download.pdf/vn-ber-d.pdf

Jona Karg
Leiter Schulungswesen

Health Info Net AG
Seidenstrasse 4
8304 Wallisellen
Telefon 0848 830 740
jona.karg[at]hin.ch
www.hin.ch