Anzeige

sinfonie®

Pflege Management

Die Zeitung für Führungskräfte
in der mobilen und stationären Pflege

10. Jahrgang
August/September 2026

Aus dem Inhalt

Zauber des Spieltisches Seite 1–2
Eine Zaubertafel projiziert mit Lichteffekten Spiele für Menschen mit Demenz auf einen Tisch. Durch Stimulationen werden so Isolationen durchbrochen und längst verloren geglaubte soziale Interaktionen wiederbelebt.

Märchen der Ökologie Seite 3
Die Europäische Union will Banken jetzt verpflichten, die Kreditvergabe an Pflegeeinrichtungen von deren ökologischer Leistungsfähigkeit abhängig zu machen. Und das ohne Finanzierungsprogramm für die Gesundheits- und Sozialwirtschaft.

Magie des Recruitings Seite 10
Neue Pflegefachkräfte durch Künstliche Intelligenz gewinnen? Das erscheint nicht nur als interessante Alternative, sondern erweist sich mittlerweile als optimaler Lösungsansatz. Das geniale Programm von Agenturgründer Giovanni Bruno liefert alles aus einer Hand und ist ein echter Game-Changer für die Personalwirtschaft in der Pflege. Für Leser der *PflegeManagement* wird die neue KI-gestützte Software sogar rabattiert. Aber nur über einen limitierten Zeitraum.

Wirkmacht der Pflege Seite 16
Unter dem Motto „#PflegeWirkt" stellt der Deutsche Pflegetag vom 12.–13.11.2026 die Rahmenbedingungen für Pflege als gestaltende Kraft in den Mittelpunkt.

Kein Jungbrunnen, aber immerhin … … ein Zaubertisch

Kegeln, Bingo, Sitzgymnastik: An Aktivitäten wie diesen können Menschen mit Demenz kaum teilhaben. Soziale Interaktionen nehmen immer mehr ab, Isolation droht. Dem wirkt die Tovertafel (niederländisch für „Zaubertisch") gezielt entgegen. Die innovative Spielkonsole wurde speziell für Menschen mit mittlerer bis fortgeschrittener Demenz entwickelt.

▶ *Fortsetzung auf Seite 2*

Gastkommentar

Strukturen, die unterstützen

Prävention neu denken – Für mehr Lebensqualität und ein tragfähiges Gesundheits- und Pflegesystem

Von Katrin Staffler, Pflegebevollmächtigte der Bundesregierung

Deutschland steht gesundheitspolitisch an einem Wendepunkt. Nur mit einer konsequenten Präventionspolitik wird unser Gesundheits- und Pflegesystem erfolgreich für alle sein. Gerade aus pflegepolitischer Perspektive ist das entscheidend: denn Prävention kann wesentlich dazu beitragen, Pflegebedürftigkeit zu vermeiden oder hinauszuzögern.

Die Fakten liegen auf dem Tisch. Rund 40 Prozent aller vermeidbaren Todesfälle in Deutschland gehen auf vier zentrale Risikofaktoren zurück: Tabak- und Alkoholkonsum, ungesunde Ernährung und Bewegungsmangel. Der aktuelle Präventionsbericht und insbesondere der Public Health Index des AOK-Bundesverbandes und des Deutschen Krebsforschungszentrums zeigen eindrücklich, dass genau hier die größten Hebel liegen – und dass Deutschland sie bislang nicht ausreichend nutzt.

Der Public Health Index macht deutlich, wie groß hier der Nachholbedarf ist: Deutschland landet im europäischen Vergleich auf einem der hinteren Plätze. Während andere Länder gezielt gegensteuern – etwa durch höhere Abgaben, Werbebeschränkungen oder verbindliche Standards für gesunde Ernährung – setzt Deutschland noch zu häufig auf Freiwilligkeit, Appelle und viel Eigeninitiative.

Katrin Staffler, Pflegebevollmächtigte der Bundesregierung.

Das reicht nicht.

Wer Prävention ernst meint, muss Prävention breiter denken und die Lebensverhältnisse verändern. Verhältnisprävention ist der Schlüssel. Denn gesundheitsschädliches Verhalten entsteht nicht allein aus individuellen Entscheidungen, sondern aus den Bedingungen, in denen Menschen leben. Wenn zuckerreiche Lebensmittel allgegenwärtig und günstig sind, wenn Alkohol gesellschaftlich normalisiert ist und

▶ *Fortsetzung auf Seite 2*

IVR Eckl GmbH • Karlstraße 69 • 50181 Bedburg

Wirtschaftsprüfung, Recht und Beratung

Digitaler Transformationsprozess in der Pflege trifft auf strukturelle Defizite der Informationssicherheit

Von Raphael Schmillenkamp, Berater, Sanovis GmbH

Digitale Pflegedokumentation, mobile Endgeräte, digitale Tourenplanung und die Anbindung an übergreifende Infrastrukturen prägen mitunter den Versorgungsalltag in der Pflege. Was Prozesse beschleunigt, Mitarbeitende entlastet und Qualität sichert, schafft zugleich neue Abhängigkeiten und Angriffsflächen. Gleichzeitig nimmt die Bedrohung im Cyberraum spürbar zu.

Während Krankenhäuser stärker in sicherheitsrechtliche Vorgaben eingebunden sind, agieren Pflegeeinrichtungen häufig in einem Zwischenraum. Sie tragen Verantwortung für besonders schutzbedürftige Daten, verfügen aber oft weder über pflegespezifische Sicherheitsstandards noch über ausreichende Ressourcen für eine belastbare Sicherheitsorganisation.

Dass diese Risiken keineswegs abstrakt sind, sondern sich bereits auf Ebene der eingesetzten Anwendungen manifestieren, zeigen Analysen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Sicherheit digitaler Pflegedokumentationssysteme. Diese zeigen, dass insbesondere in der ambulanten Pflege diverse Systeme im Einsatz sind, die wiederholt Schwachstellen aufweisen.

Gerade weil sensible Daten mobil im häuslichen Umfeld verarbeitet werden, wächst die Angriffsfläche zusätzlich. Informationssicherheit ist daher keine technische Randfrage, sondern Voraussetzung für die Stabilität einer zunehmend digitalisierten Pflege.

Pflegeeinrichtungen können diesen Anforderungen bislang vielfach nur eingeschränkt gerecht werden; ursächlich sind dabei nicht allein einzelne technische Schwachstellen, sondern tieferliegende strukturelle Defizite.

Strukturelle Defizite und ihre praktischen Folgen

Die bestehende Verwundbarkeit der Einrichtungen ist wesentlich durch strukturelle Defizite bedingt. Es fehlt an klaren Anforderungen sowie an einer angemessenen Einbindung in Sicherheitsarchitekturen, Aufsicht und Fördermechanismen. Vorgaben aus dem Krankenhausbereich lassen sich nur begrenzt auf die stationäre Langzeitpflege übertragen und noch weniger auf die ambulante Versorgung.

Zusätzlich bestehen knappe personelle und finanzielle Ressourcen, oft ohne klar definierte Verantwortlichkeiten für die Informationssicherheit, bei gleichzeitig hoher Abhängigkeit von Standardsoftware sowie externen Dienstleistern. Themen wie sicheres mobiles Arbeiten und Phishing-Prävention in der Häuslichkeit sind in Aus-, Fort- und Weiterbildung bislang nicht flächendeckend verankert.

Fachverbände kritisieren vor diesem Hintergrund die Kombination aus unklaren politischen Rahmenbedingungen, organisatorischer Überforderung und praktischen Umsetzungsproblemen. Zugleich fordern sie pflegespezifische Standards, klare Herstellerpflichten und eine verlässliche Finanzierung. Gerade wegen der weiterhin lückenhaften Rahmenbedingungen gewinnt das Handeln auf Einrichtungsebene zusätzlich an Bedeutung.

Pflegemanagement in der Verantwortung

Pflegeeinrichtungen können bestehende regulatorische Lücken nicht eigenständig schließen. Sie können jedoch innerhalb ihres Verantwortungsbereichs handlungsfähig werden und Informationssicherheit als Bestandteil professioneller Organisationsentwicklung verankern.

Erfolgversprechend ist dabei ein Ansatz, der Sicherheit nicht als befristetes Projekt, sondern als dauerhafte Querschnittsaufgabe versteht. Ein solcher Ansatz setzt Prioritäten auf Grundlage einer schlanken Risikoanalyse, bezieht die Lieferkette konsequent ein und schafft klare Rollen sowie alltagstaugliche Regelungen. Vier Handlungsfelder stehen dabei im Mittelpunkt:

Handlungsfeld 1: Informationssicherheit als Führungs- und Organisationsaufgabe

Informationssicherheit ist mehr als eine IT-Frage. Sie berührt Versorgungsqualität, Patientensicherheit, Haftung und Reputation und gehört deshalb auf die Leitungsebene. Sicherheitsaspekte sollten systematisch in Digitalisierungsentscheidungen einfließen, etwa bei der Auswahl von Dokumentationssoftware.

Wirksam wird Informationssicherheit dann, wenn sie zudem an bestehende Steuerungsstrukturen angebunden ist. Werden Risiken regelmäßig in Steuerungsgremien beraten, Vorfälle über Meldesysteme erfasst und Maßnahmen in die Jahresplanung aufgenommen, wird Sicherheit Teil der Organisationslogik, anstatt ein isoliertes IT-Thema zu bleiben.

Handlungsfeld 2: Systematische Risikoanalyse und Priorisierung

Nicht alle Risiken lassen sich gleichzeitig adressieren. Oft genügt eine schlanke, regelmäßig wiederkehrende Risikoanalyse, sofern sie an den eigenen Kernprozessen ansetzt. Zunächst sind kritische Anwendungen und Datenbestände zu identifizieren und in ihrer Bedeutung für Betrieb und Versorgung zu bewerten. Anschließend werden relevante Bedrohungen betrachtet.

Aus dieser Bewertung ergibt sich eine Prioritätenliste, die klärt, welche Systeme besonders ausfallsicher sein müssen, welche Maßnahmen kurzfristig wirksam sind und welche strukturellen Anpassungen mittelfristig geplant werden sollten. Eine jährliche Überprüfung sowie eine anlassbezogene Aktualisierung nach größeren Veränderungen tragen dazu bei, die Bewertung belastbar und aktuell zu halten.

Handlungsfeld 3: Sicherheitsorientierte Auswahl und Steuerung von IT-Dienstleistern und Systemen

Viele Einrichtungen sind auf externe IT-Dienstleister und Standardsoftware angewiesen. Damit wird die Lieferkette zugleich zum sicherheitsrelevanten Hebel und zur potenziellen Risikozone. Umso wichtiger ist es, Informationssicherheit nicht nur bei der Auswahl von Systemen und Anbietern zu berücksichtigen, sondern auch in deren laufender Steuerung zu verankern.

Raphael Schmillenkamp, Berater, Sanovis GmbH.
Raphael.schmillenkamp@sanovis.com

Sicherheitsanforderungen sollten frühzeitig definiert, transparent kommuniziert und über den gesamten Beschaffungs- und Nutzungszyklus hinweg verbindlich nachgehalten werden. Informationssicherheit in der Lieferkette erfordert damit nicht nur sorgfältige Auswahlentscheidungen, sondern vor allem eine aktive und kontinuierliche Steuerung externer Abhängigkeiten.

Handlungsfeld 4: Rollen, Verantwortlichkeiten und einfache, verbindliche Regeln

Wirksamkeit entsteht dort, wo Zuständigkeiten eindeutig sind und Regelungen den Arbeitsalltag tatsächlich erreichen. Auch in kleineren Einrichtungen sollte daher eine zentrale Ansprechperson benannt werden, die Informationssicherheitsaktivitäten koordiniert, sensibilisiert und über Entwicklungen berichtet.

Parallel dazu braucht es wenige, klare und verständliche Kernregeln. Diese sollten den Umgang mit Passwörtern und Mehrfaktor-Authentifizierung festlegen, die Nutzung privater Geräte und Datenträger regeln, Meldewege bei Verdachtsfällen beschreiben und das Verhalten bei IT-Ausfällen definieren. Wiederkehrende, praxisnahe Schulungen sowie kurze Hinweise im Arbeitsalltag erleichtern die Umsetzung und fördern die Verbindlichkeit.

Auch unter knappen personellen und finanziellen Bedingungen lassen sich wirksame Basisschutzmaßnahmen umsetzen. Entscheidend ist, mit einem pragmatischen Mindestniveau zu beginnen, das zentrale Risiken adressiert, digitale Abhängigkeiten begrenzt und die Handlungsfähigkeit im Störungsfall sichert. Gerade für Pflegeeinrichtungen kommt es darauf an, Sicherheit nicht zu überfrachten, sondern schrittweise, alltagstauglich und mit klarem Bezug zu den eigenen Versorgungsprozessen zu verankern.

Die Chancen der digitalen Pflege lassen sich nur auf einer sicheren Grundlage nutzen. Informationssicherheit ist daher keine nachgelagerte Zusatzaufgabe, sondern eine zentrale Voraussetzung für verlässliche Versorgung. Für das Pflegemanagement heißt das, Sicherheit als Führungsaufgabe zu begreifen, Risiken systematisch zu steuern, externe Abhängigkeiten bewusst zu gestalten und klare Verantwortlichkeiten in der Organisation zu verankern.

Zugleich braucht es verlässliche strukturelle Rahmenbedingungen, damit Einrichtungen dieser Verantwortung dauerhaft gerecht werden können. Erst das Zusammenspiel aus organisatorischen Maßnahmen und geeigneten externen Voraussetzungen ermöglicht eine digitale Pflegeinfrastruktur, die Versorgung stärkt, anstatt neue Verwundbarkeiten zu schaffen. ◆

Weitere Informationen:
www.sanovis.com