Interoperabel, webbasiert, zukunftssicher

Das Gemeinschaftskrankenhaus Havelhöhe setzt auf Best-of-Breed-Lösungen der United Web Solutions mit dem KIS CLINIXX von AMC im Mittelpunkt

Das Gemeinschaftskrankenhaus Havelhöhe (GKH) ist ein Akuthaus der Regelversorgung in Berlin mit rund 400 Planbetten. Seine IT hat das GKH schon früh sehr modern aufgestellt – mit Web-Technologie und Best-of-Breed-Lösungen.

Schon 2004 suchte man hier nach einem zukunftsfähigen KIS, erklärt Moritz Vorbrodt. Vor sechs Jahren kam Vorbrodt zum GKH als Organisations- und Prozessmanager und kümmert sich seitdem um die Belange von Ärzten, Pflegenden und Therapeuten in Zusammenarbeit mit der IT. „Sie alle sprechen eine unterschiedliche Sprache, betont der Organisationsmanager, „und ich vermittle zwischen den Erwartungshaltungen, etwa im Leitungskreis und den Verantwortungskreisen im Haus."

Rasch wurde 2004 den Entscheidern klar, dass die künftige Lösung zukunftsweisend sein – und daher auf Webtechnologie aufbauen – sollte. Dies war auch der explizite Wunsch des Geschäftsführers und ärztlichen Leiters Prof. Dr. med. Harald Matthes. So entschied sich das Haus für „Best-of Breed" und interoperable Lösungen – mit dem Krankenhausinformationssystem (KIS) CLINIXX® von AMC als Herzstück. Schrittweise, so Vorbrodt, erfolgte die Erweiterung durch Module aus dem Verband United Web Solutions e.V. (UWS): apenio® kam hinzu, für das Pflegemanagement mit den ganz speziellen Ansprüchen an die Dokumentation. Ein ID-Modul hatte die Unterstützung für die medizinischen Dokumentationsassistenten/innen im Kontext der Abrechnungssicherung ebenso zum Ziel wie für die Medizincontroller im MD-Kontext. Timerbee von Imilia lieferte die OP-Terminierung. medatixx übernahm das ambulante Patientenmanagement. Timerbee von Imilia folgte für die OP-Terminierung. Patientenformulare sowie entsprechende Workflows des Softwarehauses freiblick

dienen dem Onboarding und der Patientenbefragung. Transact wiederum sorgt für das professionelle Controlling und Business Intelligence auf Basis von Qlik – Neben diesen UWS-Lösungen wurden Subsysteme wie Laborinformationssystem (LIS), Radiologieinformationssystem (RIS) und Kardio-Informationssystem (CVIS) und weitere an das KIS angebunden.

Umsetzung und Betrieb

„UWS garantiert, dass die Systeme der Initiative miteinander nahtlos kommunizieren können", unterstreicht Vorbrodt. „Das funktioniert! Wenn es im Betrieb einmal ein Problem gibt, dann kümmern sich die Leute von UWS. Die Anflanschung von Softwarelösungen Dritter ist im Vergleich zu den UWS-Produkten etwas aufwändiger, und mitunter entstehen Schwierigkeiten bei der Verantwortung, wenn es hakt."

Im Betrieb erhalten Anwender den benutzerfreundlichen Eindruck, sie würden nur innerhalb eines Systems – des KIS – arbeiten. Nach der Anmeldung im KIS werden die Nutzerdaten in die anderen UWS-Systeme durchgereicht. Der Zugriff auf die UWS-Programme erfolgt über einen Fremdprogrammaufruf – ein nahtloser Vorgang, der sich für Nutzer oft wie das Weiterarbeiten innerhalb von CLINIXX anfühlt.

Diese Vorteile gibt es beim Arbeiten mit Systemen außerhalb UWS – also etwa RIS und CVIS nicht. Hier funktioniert der Datenaustausch über die Schnittstelle mit Auftrag- und Befundübermittlung gut, aber Mitarbeitende müssen sich separat anmelden, so der Organisationsmanager.

Anwendungsbeispiel Patienten-Onboarding

„Komplett papierlos arbeiten – dieses Ziel haben wir noch nicht in allen Bereichen erreicht", ist sich Vorbrodt im Klaren. „Aber wir sind auf dem guten Weg". Im Bereich der Schmerzmedizin startet demnächst ein Projekt zur Voranamnese von zu Hause aus.

„Über freiblick machen wir die Anamnese-Fragebögen online verfügbar. Den Datenschutz sichern wir dadurch, dass der Patientenbezug zum ausgefüllten Dokument durch uns im KIS hergestellt wird. Zwei-Faktor-Authentifizierung unterstützt den sicheren Ansatz." sagt Vorbrodt. Sobald der Patient ein Formular freigibt, wird es im KIS zur Verfügung gestellt. „Dieser Ansatz reduziert unseren Personalaufwand, verringert die Verweildauer und vermeidet den Eindruck bei den Patienten, dass sie allein für diesen Anamneseprozess viel Zeit im Krankenhaus verbringen müssen."

Perspektiven

Auf die Anforderungen der Telematikinfrastruktur (TI) ist das GKH bestens vorbereitet, stellt der Organisationsmanager fest. „AMC hat uns gut an die Hand genommen. Wir sind seit mehr als zwei Jahren an die TI angeschlossen – mit Aspekten wie Patientenaufnahme, VSDM, ePA, KIM, eAU usw." Alles funktioniere wunderbar, fährt Vorbrodt fort. Die GKH nimmt gemeinsam mit AMC erfolgreich am Feldtest der gematik zu eAU teil – mit dem gesamten Workflow dahinter. „Solche Engagements machen Spaß, weil man die Ansätze jetzt noch mitsteuern kann", sagt Vorbrodt.

Künftig soll im GKH auch der Core Server der United Web Solutions zum Einsatz kommen. Dadurch wird schon jetzt der interoperable Datenaustausch durch Informationssysteme im Krankenhaus (ISiK) in Konformität mit den gesetzlich verpflichtenden Vorgaben der gematik gewährleistet. Zu zahlreichen Projekten zählt ferner die Realisierung des eMedikationsplans – ebenfalls laut künftiger Spezifikation der gematik, unter Umgehung von pdfs – mit ID MEDICS, natürlich von einem UWS-Partner.

Enge Zusammenarbeit

Die Zusammenarbeit zwischen GKH und AMC sowie den Partnerfirmen aus dem Verbund der United Web Solutions (UWS) ist eng und intensiv, betont Vorbrodt: „Alle profitieren! Im Zusammenspiel entstehen tolle, tragfähige Ideen, auch im Kontext des KHZG. Dieses agile Unternehmen kennt seine Kunden sehr gut."

Anbieterunabhängige, integrierte Systeme mit CLINIXX im Zentrum: Organisations- und Prozessmanager Moritz Vorbrodt sorgt für zukunftsrobuste IT-Lösungen am Gemeinschaftskrankenhaus Havelhöhe in Berlin

Digitalisierung und IT-Sicherheit in Krankenhäusern

In 4 Schritten zum sicheren, digitalen Arbeitsplatz

Die digitale Transformation schreitet auch in Deutschlands Krankenhäusern voran. Doch was eigentlich die Patientenversorgung verbessern und eine Entlastung für die Mitarbeiter sein soll, kann ohne gezielte Unterstützung schnell im Gegenteil münden. Denn auf ihrem Digitalisierungsweg sind Krankenhäuser gleich mit mehreren Herausforderungen konfrontiert. Wie es dennoch gelingt, einen sicheren, digitalen Arbeitsplatz zu schaffen, erläutert Manuel Sosna der ISEC7 Group.

Von Manuel Sosna, Sales Director, ISEC7 Group

Herausforderungen für die Digitalisierung von Krankenhäusern

Mit dem Krankenhauszukunftsfond (KHZF) hat die Bundesregierung über vier Milliarden Euro zur Verfügung gestellt, um Krankenhäusern ein digitales Update zu ermöglichen. Bedingung ist, dass die Krankenhäuser 15 Prozent der beantragten Mittel für die IT-Sicherheit einsetzen und zudem die konkreten Fortschritte bei der digitalen Infrastruktur und IT-Sicherheit nachweisen können. Allein die Analyse des Ist-Zustands durchzuführen, Ansatzpunkte auf Basis der Fördertatbestände zu erarbeiten und schließlich einen Antrag zu stellen, ist für viele Krankenhäuser eine Mammutaufgabe. Kein Wunder, dass ein Großteil des Fördergeldes bislang unangetastet bleibt. Hinzu kommt der Mangel an IT-Fachpersonal. Das und zunehmende Cyberattacken, auch im Gesundheitssektor, sind eine beunruhigende Entwicklung. So verzeichnet der diesjährige Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) 14,8 Millionen Meldungen zu Schadprogramm-Infektionen. Das sind doppelt so viel wie im Jahr zuvor. Insbesondere die Angriffe mit Ransomware werden immer ausgefeilter und damit gefährlicher. Infolge einer solchen Cyberattacke konnte etwa das Universitätsklinikum Düsseldorf 13 Tage lang keine Notfall-Patienten aufnehmen. Zugleich haben Krankenhäuser mit einem steigenden Kostendruck und der damit einhergehenden Notwendigkeit zur Effizienzsteigerung zu kämpfen.

4 Schritte für einen sicheren, digitalen Arbeitsplatz im Krankenhaus

Fakt ist, dass sich das Fortschreiten der Digitalisierung nicht aufhalten lässt. Dabei gibt es Mittel und Wege, um die genannten Herausforderungen zu überwinden. Vier Schritte zeigen, wie Krankenhäuser einen sicheren, digitalen Arbeitsplatz schaffen:

1. Schritt: Denken Sie frühzeitig an die IT-Sicherheit.

IT-Sicherheit nimmt einen immer größeren Stellenwert ein, sodass sie die Grundlage Ihres Digitalisierungsprojekts, im Sinne einer sicheren Digitalisierung, bilden sollte. Dazu gehört, konventionelle Virenschutzsoftware durch Lösungen, die auf Künstlicher Intelligenz (KI) basieren, abzulösen. Die Vorteile eines solchen Endgeräteschutzes sind, dass Bedrohungen zuverlässig identifiziert und blockiert werden, bevor sie überhaupt Schaden anrichten können. Eine KI-basierte Lösung schaut nicht nur voraus, sie lernt auch stetig dazu und bietet automatisierte Erkennungs- sowie Reaktionsmöglichkeiten, die Krankenhäuser optimal schützen.

2. Schritt: Setzen Sie auf eine zentrale Verwaltung.

Um die IT-Sicherheit in Krankenhäusern noch weiter zu stärken, ist es unabdingbar, dass Endgeräte-Sicherheit und -Management stärker zusammenwachsen. Anstatt Ärzte und Pflegepersonal die Devices selbst verwalten zu lassen, gilt es, diese in ein Unified-Endpoint-Management-System (UEM) einzubinden. Das dämmt nicht nur Schatten-IT ein, sondern verhindert zugleich Sicherheitslücken. Innerhalb einer einheitlichen Oberfläche lassen sich so plattformübergreifende Routineaufgaben, wie Betriebssystem- und Softwareinstallation, Patch- und Lizenzmanagement sowie mobile Geräte, Desktops und Anwendungen verwalten. Idealerweise wird das UEM-System um ein Monitoring aller kritischen Endpunkte ergänzt und mit zusätzlichen Services wie Kostenverrechnung und 24/7 Support erweitert.