Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt



WISSEN

Alle Beiträge der Serie zu Microsoft 365 im Krankenhaus an einem Ort.

› **Microsoft 365 im Krankenhaus**

BERATUNG

Grenze zwischen KIS und Microsoft 365 ziehen, Purview-Leitplanken planen, Verfahrensanweisung mit dem Datenschutz abstimmen.

› **Beratung für Krankenhäuser**

SCHULUNG

Für Klinik-IT, Datenschutz und QM: Vertraulichkeitsbezeichnungen, DLP und sichere Zusammenarbeit in Teams und SharePoint.

› **Schulung für Krankenhäuser**

Es gibt in fast jedem Krankenhaus eine Datei, die niemand offiziell kennt und ohne die trotzdem keine Station durch den Tag kommt. Sie heißt etwa „Belegung_aktuell_FINAL_v7_NICHT_LÖSCHEN.xlsx“, liegt in einem Teams-Kanal, hat vierzehn Bearbeiter und eine Spalte „Bemerkung“, in der Dinge stehen, die eigentlich in die Patientenakte gehören. Wenn Sie jetzt kurz an eine ganz bestimmte Datei denken mussten: Willkommen, Sie sind hier richtig.

Die Grundhaltung dieses Beitrags ist schnell erzählt. Behandlungsdokumentation gehört ins KIS und in seine Subsysteme, also LIS, RIS, PACS und das OP-Management. Microsoft 365 ist im Krankenhaus ein Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Das klingt nach einer sauberen Linie. In der Realität ist es eher ein Gartenzaun mit Lücken, durch die jeden Tag Belegungslisten, OP-Pläne, Arztbriefe, Wundfotos und Tumorkonferenz-Unterlagen schlüpfen. Nicht, weil Ärzte und Pflegekräfte den Datenschutz verachten, sondern weil das KIS an genau dieser Stelle eine Funktion nicht hat, zu langsam ist oder nicht auf das Gerät passt, das gerade in der Kitteltasche steckt.

Dieser Beitrag nimmt die fünf häufigsten Grauzonen auseinander: warum sie entstehen, welches Risiko sie tragen und wie die saubere Lösung aussieht. Danach geht es um die technischen Leitplanken in Microsoft 365, also Vertraulichkeitsbezeichnungen, DLP-Regeln, eingeschränkte Sites und gesperrten Gastzugriff, und um die Organisation drumherum. Er richtet sich an IT-Leitungen und Administratoren, Geschäftsführungen, Informationssicherheits-, Datenschutz- und Qualitätsmanagementbeauftragte, die Medizintechnik sowie an Betriebsräte, Personalräte und Mitarbeitervertretungen. Arztpraxen, Pflegeheime und Krankenkassen haben andere Rahmenbedingungen und sind hier nicht gemeint.

FAKTEN · Das Wichtigste in Kürze

Behandlungsdokumentation gehört ins KIS. Microsoft 365 ist kein Ersatz für die Patientenakte, auch nicht für ein paar Tage.

Fast jede Grauzone hat eine Ursache im Alltag: eine fehlende KIS-Funktion, ein fehlender mobiler Zugang, ein umständlicher Versandweg. Wer nur verbietet, verschiebt das Problem auf private Smartphones.

Microsoft 365 bringt Leitplanken mit: Vertraulichkeitsbezeichnungen, DLP-Regeln, eingeschränkte Sites, Gastzugriffssteuerung, App-Schutz. Sie wirken nur zusammen und nur mit klarer Regel im QM-Handbuch.

Ob und wie Patientendaten in einem Cloud-Dienst verarbeitet werden dürfen, entscheidet der Verantwortliche gemeinsam mit dem Datenschutzbeauftragten. Dieser Beitrag ersetzt keine Rechtsberatung.

Die Grenzlinie: Was ins KIS gehört und was Microsoft 365 kann

Behandlungsdokumentation ist KIS-Sache

Das Bürgerliche Gesetzbuch verpflichtet in § 630f BGB Ärzte und Krankenhaus als Behandler, eine Patientenakte zu führen, Änderungen nachvollziehbar zu halten und die Akte über Jahre aufzubewahren. Dafür gibt es im Krankenhaus das KIS: mit Fallbezug, Rollen- und Berechtigungskonzept, Protokollierung jedes Zugriffs, Schnittstellen zu Labor, Radiologie und Abrechnung und mit einem Hersteller, der für genau diesen Zweck geprüft wird. Ein Teams-Kanal kann vieles, aber er weiß nicht, welcher Fall zu welchem Patienten gehört, wer gerade behandelnd ist und wann die Aufbewahrungsfrist einer Akte abläuft.

Daraus folgt die erste und wichtigste Regel: Alles, was Teil der Behandlung ist, also Befunde, Anordnungen, Verläufe, Bilder, Briefe und Pflegedokumentation, entsteht im KIS oder in einem angebundenen Subsystem und bleibt dort. Was in Microsoft 365 landet, ist im besten Fall eine Kopie, im schlechtesten die einzige Fassung. Beides ist schlechter als das Original im KIS.

Was Microsoft 365 im Krankenhaus gut kann

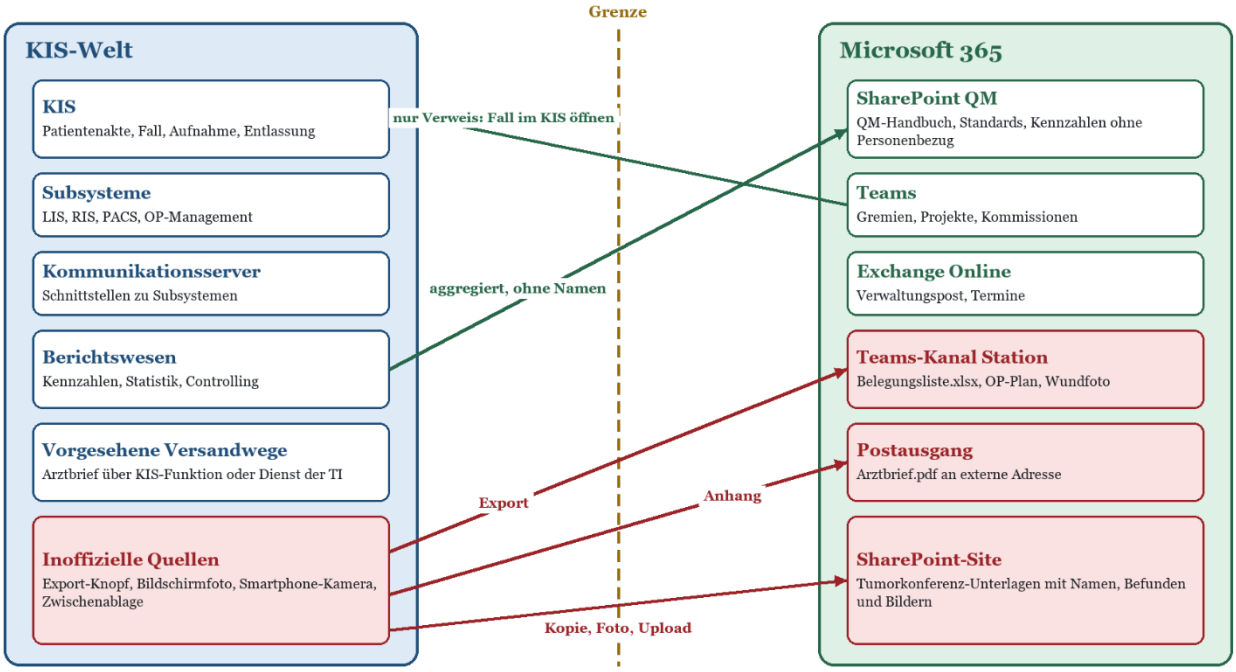
Die Stärken liegen auf der anderen Seite der Linie: Gremienarbeit in Teams, Projektarbeit, Kommissionen, die Hygienekommission ebenso wie die Arzneimittelkommission, das QM-Handbuch mit Verfahrensanweisungen und Standards in SharePoint, die Verwaltungspost in Exchange, Dienstbesprechungen per Videokonferenz, Kennzahlen ohne Personenbezug für die Geschäftsführung. Für all das ist Microsoft 365 im Krankenhaus ein ausgesprochen gutes Werkzeug. Warum die Klinik dabei anders tickt als Verwaltung und Mittelstand, beschreibt der Grundlagenbeitrag Microsoft 365 im Krankenhaus: Warum die Klinik anders tickt als Verwaltung und Mittelstand. Den Überblick über alle Themen der Serie finden Sie auf der Übersichtsseite Microsoft 365 im Krankenhaus.

Warum die Grenze trotzdem durchlässig ist

Die Lücken im Zaun entstehen fast nie aus Leichtsinn. Sie entstehen, weil das KIS in einem bestimmten Moment nicht das liefert, was der Alltag braucht: eine Übersicht über alle Stationen auf einen Blick, eine Liste, die man in der Frühbesprechung an die Wand werfen kann, ein Foto, das der Oberarzt in der Rufbereitschaft sofort sieht, einen Brief, der heute noch beim Nachversorger sein muss. Microsoft 365 ist dann einfach da, auf jedem Rechner, auf jedem Diensthandy, und es funktioniert. Genau das macht es gefährlich.

Datenflüsse zwischen KIS und Microsoft 365

Grün: vorgesehene Wege. Rot: Wege, die im Alltag entstehen und die niemand bestellt hat.



Skizze: Die grünen Pfade tragen Kennzahlen und Verweise, die roten tragen Patienten. Ziel ist, die roten auszutrocknen.

Die Skizze zeigt das Prinzip. Grüne Pfade sind solche, die man bewusst einrichtet: Aggregierte Kennzahlen aus dem Berichtswesen wandern in den QM-Bereich, und aus Microsoft 365 heraus gibt es höchstens einen Verweis nach dem Muster „Fall im KIS öffnen“, ohne dass Patientendaten selbst die Seite wechseln. Rote Pfade sind Export, Anhang, Kopie und Foto. Sie sind technisch trivial, deshalb gibt es sie überall.

Datenart	Beispiele	Gehört nach
Behandlungsdokumentation	Befunde, Anordnungen, Verlauf, Pflegedokumentation, Arztbrief	KIS und Subsysteme
Medizinische Bilder	Röntgen, CT, Wundfotos, Endoskopie	PACS oder KIS-Bildablage
Organisatorisches mit Patientenbezug	Belegung, OP-Reihenfolge, Transportliste	KIS-Funktion, sonst Grauzone mit Freigabe
Organisatorisches ohne Patientenbezug	Dienstplanabsprachen, Projektpläne, Gremienprotokolle	Microsoft 365
Qualitätsmanagement	QM-Handbuch, Verfahrensanweisungen, Standards, Hygieneplan	Microsoft 365 (SharePoint)
Kennzahlen	Fallzahlen, Verweildauer, Auslastung, aggregiert	Microsoft 365, wenn kein Rückschluss auf Personen möglich ist

Die fünf Grauzonen: Ursache, Risiko, saubere Lösung

Die folgenden fünf Fälle tauchen so oder ähnlich in vielen Häusern auf. Sie sind bewusst nicht als Anklage gemeint. Wer sie im eigenen Haus wiederfindet, hat kein Versagen entdeckt, sondern einen Arbeitsauftrag, und zwar meistens einen an das KIS.



Skizze: Verbote treffen Glied 4 und 5. Wirksam ist, die Lücke in Glied 1 zu schließen.

Belegungslisten in Excel

Warum sie entsteht: Das Bettenmanagement im KIS zeigt die Belegung oft nur pro Station oder nur in einer Maske, die sich schlecht drucken und noch schlechter in der Frühbesprechung zeigen lässt. Also exportiert jemand eine Liste, ergänzt Spalten für Isolationshinweise, geplante Entlassungen und „Sonstiges“ und legt sie dorthin, wo alle sie finden: in einen Teams-Kanal oder auf ein Netzlaufwerk, das inzwischen in OneDrive synchronisiert wird.

Risiko: Die Liste enthält Namen, Geburtsdaten, Zimmernummern und in der Spalte „Sonstiges“ gern Gesundheitsangaben. Sie ist für das ganze Team sichtbar, auch für die Schreibkraft aus einem anderen Bereich, die vor zwei Jahren einmal hinzugefügt wurde. Es gibt Versionen, Kopien in Downloads-Ordnern und Ausdrucke. Und niemand weiß, welche Fassung gilt, wenn die Liste und das KIS sich widersprechen.

Saubere Lösung: Die Belegungsübersicht kommt aus dem KIS, notfalls als Bericht oder Dashboard, das der KIS-Hersteller oder das Berichtswesen liefert, angezeigt auf einem Bildschirm im Dienstzimmer. Wenn Microsoft 365 eine Rolle spielt, dann mit aggregierten Zahlen ohne Namen: freie Betten je Station, Isolationszimmer belegt ja oder nein.

OP-Planung im Teams-Kanal

Warum sie entsteht: Die OP-Planung im Subsystem ist für die Planung selbst gebaut, nicht für die Abstimmung zwischen Chirurgie, Anästhesie, Pflege und Bettenmanagement am Vortag. Also wird der Plan als Bildschirmfoto oder Tabelle in einen Kanal gepostet, und die Diskussion läuft in den Antworten: „Kann Herr M. in Saal 3 vorgezogen werden?“

Risiko: Patientenbezug mit Eingriffsart in einem Kanal, dessen Mitgliederliste niemand pflegt, dazu Benachrichtigungen auf privaten Smartphones und eine Chat-Historie, die länger lebt als jede OP-Planung. Änderungen im Kanal erreichen das OP-Management nicht zuverlässig. Damit gibt es zwei Wahrheiten, und im OP ist das keine akademische Frage.

Saubere Lösung: Abstimmung im Kanal ja, Patientendaten nein. Im Kanal steht „Saal 3, Position 2 vorziehen, Details im OP-Plan“. Wer den Patienten wissen muss, hat Zugriff auf das OP-Management. Wenn diese Disziplin nicht trägt, braucht das Subsystem eine Abstimmungsfunktion oder eine Lesesicht, und das ist eine Anforderung an den Hersteller.

Arztbriefe als Mail-Anhang

Warum sie entsteht: Der vorgesehene Versandweg aus dem KIS ist umständlich, beim Empfänger nicht eingerichtet oder hat eine Störung. Der Nachversorger ruft an, der Brief muss raus, also wird er als PDF exportiert und per Outlook verschickt. An eine Adresse, die jemand am Telefon buchstabiert hat.

Risiko: Ein Tippfehler in der Adresse, und der Arztbrief liegt bei einem Fremden. Der Brief liegt außerdem zusätzlich in „Gesendete Elemente“, im Postfach des Empfängers und je nach Konfiguration unverschlüsselt auf dem Transportweg. Das ist der klassische Weg zu einer meldepflichtigen Datenpanne.

Saubere Lösung: Der Versand läuft über den Weg, den das KIS vorsieht, etwa über einen Dienst der Telematikinfrastruktur, wenn das Haus und der Empfänger ihn nutzen. Wo E-Mail im Ausnahmefall bleibt, greift eine DLP-Regel, die externe Mails mit typischen Patientenmerkmalen blockiert oder nur verschlüsselt zulässt, und eine Verfahrensanweisung regelt, wer die Ausnahme freigibt.

Wundfotos im Chat

Warum sie entsteht: Die Wundexpertin will den Verlauf zeigen, der Oberarzt ist in der Rufbereitschaft zu Hause, das KIS hat keine mobile Fotoerfassung oder sie ist auf Station nicht eingerichtet. Das Diensthandy hat eine Kamera und Teams. Das Problem löst sich in dreißig Sekunden, und genau darin liegt das Problem.

Risiko: Das Foto liegt in der Kamerarolle, im Chat, im OneDrive des Absenders und eventuell in einer privaten Cloud-Sicherung des Handys. Es fehlt in der Patientenakte, obwohl es zur Behandlung gehört. Bei Privatgeräten kommt hinzu, dass die Klinik das Bild weder löschen noch herausgeben kann. Und ein Wundfoto ist eines der intimsten Dinge, die ein Krankenhaus über einen Menschen speichert.

Saubere Lösung: Fotos entstehen in einer App, die direkt in KIS oder PACS speichert, auf verwalteten Geräten. Bis es diese App gibt: Diensthandys mit App-Schutzrichtlinien, die das Speichern in die Kamerarolle und das Weitergeben an nicht verwaltete Apps unterbinden, plus eine klare Regel, dass das Foto nach Übernahme in die Akte gelöscht wird. Private Smartphones sind für Patientenfotos tabu, ohne Ausnahme.

Tumorkonferenz-Unterlagen in SharePoint

Warum sie entsteht: An einer Tumorkonferenz sitzen mehrere Fachabteilungen, oft auch externe Ärzte aus Kooperationspraxen oder anderen Häusern des Klinikverbunds. Die Vorbereitung braucht eine Fallliste, Befunde und Bilder an einem Ort, und die KIS-Funktion für Konferenzen fehlt, ist nicht standortübergreifend oder bindet externe Teilnehmer nicht an. Also entsteht eine SharePoint-Site oder ein Team, in das die Unterlagen hochgeladen werden, und die Externen werden als Gäste eingeladen.

Risiko: Hier kommt alles zusammen: besonders schutzwürdige Gesundheitsdaten, viele Teilnehmer, Gastkonten, deren Lebensdauer niemand überwacht, und eine Site, die nach Jahren eine vollständige Schattenakte zahlreicher Patienten enthält. Mit Copilot oder der organisationsweiten Suche wird so eine Site zudem schnell sichtbarer als gedacht, wenn die Berechtigungen nicht stimmen.

Saubere Lösung: Erste Wahl ist die Konferenzfunktion des KIS oder eine dafür vorgesehene Lösung mit Anbindung an die Akte. Wenn das Haus für einen Übergangszeitraum mit Microsoft 365 arbeitet, dann nur nach Freigabe durch Verantwortlichen und Datenschutzbeauftragten, in einer eingeschränkten Site mit Vertraulichkeitsbezeichnung, ohne Gäste, mit festgelegter Löschfrist nach der Konferenz und mit der Übernahme des Beschlusses in die Akte als einzig gültiger Fassung.

WARNUNG · Private Messenger sind keine Grauzone, sondern ein Loch

Wer Teams und Diensthandys verbietet, ohne die Ursache zu beheben, bekommt nicht weniger Patientenfotos, sondern Patientenfotos in privaten Messengern. Dort hat die Klinik weder Löschung

noch Protokoll noch Zugriff bei einer Auskunftsanfrage. Ein kontrollierter Weg in Microsoft 365 ist im Zweifel das kleinere Übel, aber nur als Brücke, nicht als Ziel.

Die Übersicht: Grauzone, Ursache, Risiko, bessere Lösung

Grauzone	Warum sie entsteht	Risiko	Bessere Lösung
Belegungsliste in Excel	Belegungsübersicht im KIS nicht stationsübergreifend oder nicht präsentierbar	Namen und Gesundheitsangaben für zu viele sichtbar, konkurrierende Fassungen	Bericht oder Dashboard aus dem KIS; in Microsoft 365 nur aggregierte Zahlen
OP-Planung im Teams-Kanal	Subsystem plant, unterstützt aber keine Abstimmung zwischen Berufsgruppen	Zwei Wahrheiten, Patientenbezug im Kanal, Benachrichtigung auf Privatgeräten	Abstimmung ohne Patientendaten, Verweis auf das OP-Management, Anforderung an den Hersteller
Arztbrief als Mail-Anhang	Versandweg aus dem KIS umständlich oder beim Empfänger nicht verfügbar	Fehlversand, Kopien in Postfächern, Datenpanne	Versand über KIS-Funktion; DLP blockiert externe Mails mit Patientenmerkmalen
Wundfoto im Chat	Keine mobile Fotoerfassung mit Anbindung an die Akte	Foto fehlt in der Akte, Kopien auf Geräten und in privater Sicherung	Foto-App mit Speicherung in KIS oder PACS; App-Schutz auf Diensthandys
Tumorkonferenz in SharePoint	Konferenzfunktion fehlt oder bindet externe Teilnehmer nicht an	Schattenakte, Gastkonten, Sichtbarkeit über Suche und Copilot	KIS-Konferenzlösung; übergangsweise eingeschränkte Site, keine Gäste, Löschfrist

TYPISCHE SITUATION · Weitere Kandidaten, die gern übersehen werden

Übergabezettel, die aus dem KIS gedruckt, abfotografiert und im Chat geteilt werden. Beschwerden mit Patientennamen im allgemeinen QM-Postfach. Fallbesprechungen in Besprechungsaufzeichnungen und Transkripten. Haftpflichtvorgänge im Ordner der Rechtsabteilung, der für die halbe Verwaltung freigegeben ist. Die Logik ist jedes Mal dieselbe: Ursache finden, Risiko benennen, Weg zurück ins KIS oder in einen geschützten Bereich bauen.

Technische Leitplanken in Microsoft 365

Keine Technik macht aus Microsoft 365 eine Patientenakte, und keine Technik verhindert jeden Fehler. Was die Werkzeuge leisten: Sie machen den falschen Weg mühsamer, den richtigen bequemer und beides sichtbar. Die meisten Bausteine stammen aus Microsoft Purview, ergänzt um SharePoint, Teams und Microsoft Entra ID. Welche Funktion in welchem Lizenzplan enthalten ist, ändert sich regelmäßig. Prüfen Sie das für Ihren Tenant vor der Planung anhand der aktuellen Microsoft-Dokumentation.



Skizze: Die Schichten ergänzen sich. Regel, Schulung und die Anforderung an den KIS-Hersteller ersetzen keine davon.

Vertraulichkeitsbezeichnungen

Vertraulichkeitsbezeichnungen, in Purview als Sensitivity Labels bekannt, wirken auf zwei Ebenen. Auf Dateien und E-Mails kennzeichnen sie den Inhalt, können ihn verschlüsseln und den Zugriff auf eine Gruppe beschränken, auch wenn die Datei irgendwann als Anhang das Haus verlässt. Auf Teams, Microsoft-365-Gruppen und SharePoint-Sites steuern sie als Container-Bezeichnung, ob Gäste erlaubt sind, wie freigegeben werden darf und ob nicht verwaltete Geräte überhaupt Zugriff bekommen.

Für ein Krankenhaus reichen drei bis vier Stufen. Mehr verwirrt Ärzte und Pflegekräfte, die zwischen Visite und Aufnahme keine Taxonomie studieren. Ein bewährtes Schema:

Bezeichnung	Bedeutung	Technische Wirkung
Öffentlich	Freigegeben für Presse, Website, Patienteninformation	Keine Einschränkung
Intern	Standard für Verwaltung, QM, Gremien	Keine Gäste ohne Begründung, Freigabe nur intern
Vertraulich	Personalvorgänge, Verträge, Vorstandsunterlagen	Verschlüsselung, keine Gäste, nur verwaltete Geräte
Patientenbezug	Freigegebene Ausnahmen mit Patientendaten	Verschlüsselung, eingeschränkte Site, keine Gäste, kein Download auf nicht verwaltete Geräte, Löschfrist

Die oberste Stufe heißt bewusst nicht „Streng vertraulich“, sondern beim Namen, worum es geht. Wer eine Datei so kennzeichnen will, soll merken, dass er gerade eine Ausnahme macht.

DLP-Regeln für typische Patientenmerkmale

Data Loss Prevention erkennt Inhalte anhand vertraulicher Informationstypen und reagiert darauf: mit einem Hinweis an den Benutzer, mit einer Begründungspflicht oder mit einer Sperre. Microsoft liefert viele Informationstypen mit, darunter deutsche Ausweis-, Pass- und Steuernummern sowie medizinische Begriffslisten wie Krankheiten, Medikamente, Laborbegriffe und ICD-10-CM-Codes. Eine eingebaute Erkennung für die deutsche Krankenversichertennummer findet sich in der Liste der Informationstypen dagegen nicht, und die medizinischen Begriffslisten sind nicht auf deutsche

klinische Sprache zugeschnitten. Prüfen Sie den aktuellen Stand in der Microsoft Learn: Definitionen der vertraulichen Informationstypen, bevor Sie sich darauf verlassen.

Im Krankenhaus lohnen deshalb eigene Informationstypen, die das Haus selbst kennt:

- **Krankenversichertennummer:** ein Buchstabe gefolgt von neun Ziffern, kombiniert mit Schlüsselwörtern wie „Versichertennummer“ oder „KVNR“ in der Nähe, um Fehltreffer zu senken.
- **Fall- und Patientennummern des Hauses:** Format und Präfix kennt die KIS-Abteilung. Kombiniert mit einem Datum im Geburtsdatumsformat ergibt das einen starken Treffer.
- **Schlüsselwortlisten:** Begriffe wie „Diagnose“, „Befund“, „Aufnahmedatum“, „Station“ und „geb.“ als unterstützende Hinweise, nie als alleiniges Kriterium.
- **Dokumentvorlagen aus dem KIS:** Arztbriefe und Berichte haben feste Kopfzeilen. Ein Fingerabdruck dieser Vorlage erkennt exportierte Briefe zuverlässiger als jede Wortliste.

Die Wirkung staffeln Sie nach Risiko: In internen Kanälen zunächst nur ein Richtlinientipp, der freundlich erklärt, warum diese Liste hier nicht hingehört. Beim Versand an externe Empfänger und beim Teilen mit Gästen eine Sperre mit Begründungsmöglichkeit für freigegebene Ausnahmen.

TIPP · DLP erst im Simulationsmodus laufen lassen

Starten Sie jede neue Regel im Simulationsmodus und werten Sie die Treffer einige Wochen aus, gemeinsam mit dem Datenschutzbeauftragten. Sie erfahren dabei mehr über die tatsächlichen Datenflüsse im Haus als aus jedem Interview. Und Sie vermeiden, dass die erste scharfe Regel am Montagmorgen die Entlassbriefe der Inneren blockiert und das Telefon der IT-Hotline bis mittags nicht mehr stillsteht.

Eingeschränkte Sites

Der eingeschränkte Websitezugriff in SharePoint, Teil von SharePoint Advanced Management, begrenzt den Zugriff auf eine Site auf Mitglieder bestimmter Microsoft-365-Gruppen oder Entra-Sicherheitsgruppen. Wer nicht in der Gruppe ist, kommt nicht hinein, selbst wenn er früher Berechtigungen oder einen Freigabelink bekommen hat. Laut Microsoft beachten auch die organisationsweite Suche und Copilot diese Einschränkung. Ein Detail, das gern übersehen wird: Private und freigegebene Kanäle in Teams haben eigene Sites und müssen separat eingeschränkt werden. Die Details beschreibt der Artikel Microsoft Learn: Eingeschränkter Websitezugriff in SharePoint.

Für die wenigen freigegebenen Ausnahmen mit Patientenbezug ist das die passende Hülle: eine Gruppe, die von einer verantwortlichen Person gepflegt wird, idealerweise mit regelmäßiger Zugriffsüberprüfung in Microsoft Entra ID.

Gastzugriff sperren

Gäste sind in vielen Klinik-Tenants der Weg, über den Patientendaten das Haus verlassen, ohne dass jemand eine Mail schreibt. Die Einstellung ist auf mehreren Ebenen zu treffen: Gastzugriff in Teams, externe Freigabe in SharePoint und OneDrive pro Site und organisationsweit, Einladungseinstellungen in Entra ID. Am elegantesten erledigt das die Container-Bezeichnung: Ein Team mit der Bezeichnung „Patientenbezug“ lässt keine Gäste zu, egal was der Besitzer gerne hätte. Für Gremien mit externen Mitgliedern, etwa Kooperationspartner in einer Kommission, gibt es eigene Teams ohne Patientenbezug.

Geräte, Protokoll und was sonst noch zählt

Auf Diensthandys verhindern App-Schutzrichtlinien, dass Inhalte aus Teams oder Outlook in nicht verwaltete Apps kopiert oder in der Kamerarolle gespeichert werden. Das Überwachungsprotokoll in Purview zeigt, wer wann auf welche Datei zugegriffen hat, und Aufbewahrungsrichtlinien sorgen dafür, dass freigegebene Ausnahmen nach Ablauf der Frist auch wirklich verschwinden. Wie Sie das Gesamtpaket absichern, beschreibt der Kompetenzbereich Microsoft 365 Security.

Leitplanke	Was sie leistet	Wo sie endet
Vertraulichkeitsbezeichnung	Kennzeichnet, verschlüsselt, steuert Gäste und Freigaben für Container	Nur so gut wie die Disziplin bei der Vergabe; automatische Vergabe braucht verlässliche Erkennung
DLP-Regel	Erkennt Patientenmerkmale, warnt oder blockiert	Fotos ohne Text und handschriftliche Notizen erkennt sie nicht zuverlässig
Eingeschränkte Site	Zugriff nur für definierte Gruppe, auch in Suche und Copilot	Private und freigegebene Kanäle separat; Gruppenpflege ist Daueraufgabe
Gastzugriff gesperrt	Keine externen Konten in sensiblen Bereichen	Externe Zusammenarbeit muss anders organisiert werden
App-Schutz und Protokoll	Begrenzt Abfluss auf Geräten, macht Zugriffe nachvollziehbar	Private Geräte ohne Verwaltung bleiben außen vor; Auswertung ist mitbestimmungspflichtig

FAKTEN · Copilot und Patientendaten

Copilot sieht, was der Benutzer sehen darf. Liegt eine Belegungsliste in einem Team, auf das die halbe Verwaltung Zugriff hat, kann Copilot sie bei einer harmlosen Frage nach „aktuellen Zahlen der Station“ heranziehen. Wer Copilot einführt, räumt deshalb zuerst die Grauzonen auf, nicht danach. Hintergründe beschreibt der Kompetenzbereich Microsoft 365 Copilot.

Organisation, Rechtsrahmen und Mitbestimmung

Eine Verfahrensanweisung statt hundert Einzelfallentscheidungen

Technik ohne Regel erzeugt Frust. Die Regel gehört ins QM-Handbuch, als Verfahrensanweisung „Umgang mit Patientendaten außerhalb des KIS“, gelenkt wie jedes andere Dokument. Sie benennt den Grundsatz, die zulässigen Ausnahmen mit ihren Bedingungen, den Freigabeweg über den Verantwortlichen und den Datenschutzbeauftragten, die Löschfristen und den Weg, eine fehlende KIS-Funktion als Anforderung zu melden. Wie Dokumentenlenkung in SharePoint aussieht, die im Zertifizierungsaudit nach KTQ oder ISO 9001 hält, beschreibt Dokumentenlenkung nach ISO 9001.

TYPISCHE SITUATION · Aus der Projektarbeit

Beim Aufbau eines QM-Handbuchs mit SharePoint für ein Krankenhaus war eine der ersten Entscheidungen, was nicht hineingehört. Verfahrensanweisungen, Standards und Formularvorlagen ja, ausgefüllte Formulare mit Patientenbezug nein. Diese Grenze einmal sauber zu ziehen und in der Struktur abzubilden, hat später viele Einzeldiskussionen erspart.

Der Rechtsrahmen in Kürze

Gesundheitsdaten sind besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO. Für Ärzte und ihre Gehilfen gilt zusätzlich die strafbewehrte Schweigepflicht nach § 203 StGB, die bei

der Einbindung von Dienstleistern eigene Anforderungen stellt. Hinzu kommt Landesrecht: Die Landeskrankenhausgesetze regeln den Umgang mit Patientendaten unterschiedlich, manche sehr detailliert, manche kaum, und für öffentliche Häuser gelten die jeweiligen Landesdatenschutzgesetze. Kirchliche Häuser unterliegen dem KDG oder dem DSG-EKD. Ein Bundesland als Normalfall gibt es nicht.

Für Cloud-Dienste ist § 393 SGB V einschlägig. Seit dem 1. Juli 2025 verlangt er für die Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computing unter anderem ein aktuelles C5-Typ-2-Testat der datenverarbeitenden Stelle oder ein gleichwertiges Testat beziehungsweise Zertifikat, dazu angemessene technische und organisatorische Maßnahmen und Anforderungen an den Ort der Verarbeitung. Welche Microsoft-Dienste von welchem C5-Testat welchen Typs erfasst sind, ist ein Prüfauftrag für Ihr Haus: Die Berichte stehen im Microsoft Service Trust Portal bereit, und die Prüfung gehört dokumentiert. Für die IT-Sicherheit insgesamt gilt § 391 SGB V in der Fassung des NIS2-Umsetzungsgesetzes, für Betreiber kritischer Anlagen stattdessen das BSIG. Der branchenspezifische Sicherheitsstandard „Medizinische Versorgung“ der DKG liegt in Version 1.3.1 vom 10. Oktober 2025 vor. Wie sich die Pflichten technisch in Microsoft 365 übersetzen lassen, zeigt NIS2 technisch umsetzen mit Microsoft 365.

HINWEIS · Keine Rechtsberatung

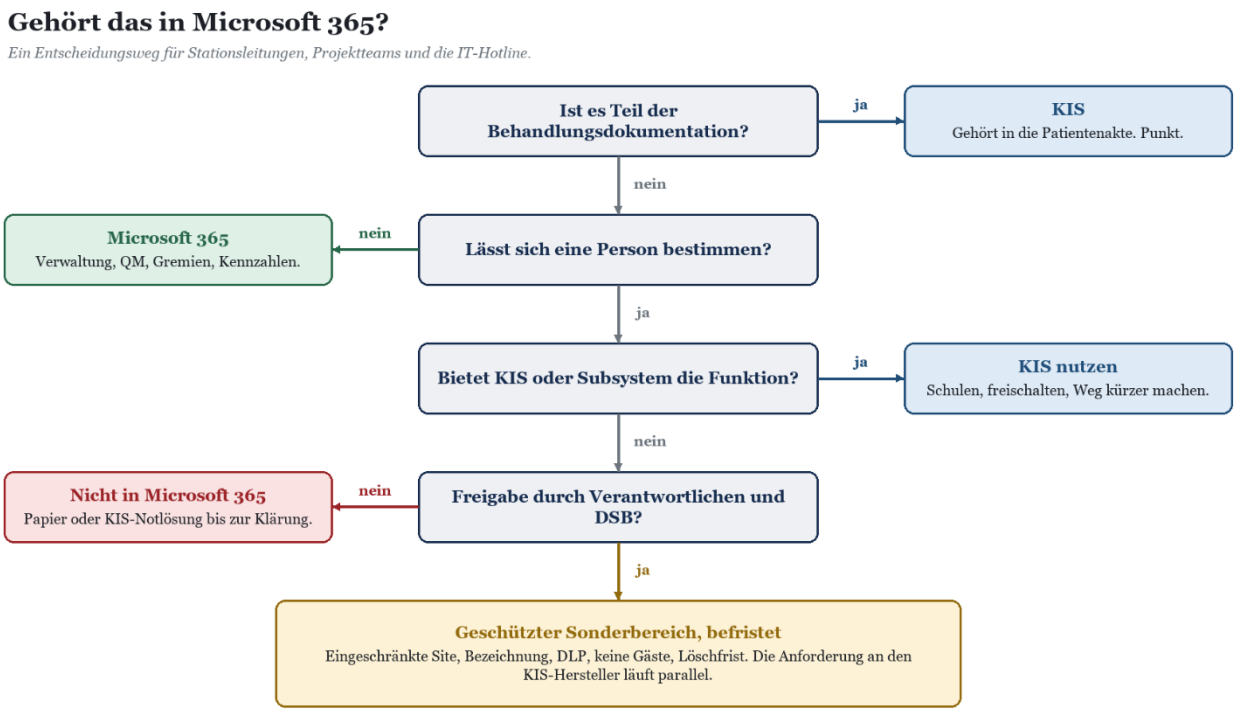
Dieser Beitrag beschreibt technische und organisatorische Möglichkeiten. Er ist keine Rechtsberatung und ersetzt keine Prüfung im Einzelfall. Ob Patientendaten in einem bestimmten Microsoft-365-Dienst verarbeitet werden dürfen, entscheidet der Verantwortliche, also in der Regel die Geschäftsführung des Krankenhauses, gemeinsam mit dem Datenschutzbeauftragten und unter Berücksichtigung des für Träger und Bundesland geltenden Rechts.

Mitbestimmung nicht vergessen

DLP-Berichte, Überwachungsprotokolle und Zugriffsauswertungen sind technische Einrichtungen, die Verhalten und Leistung der Mitarbeiterinnen und Mitarbeiter erfassen können. Im privaten Krankenhaus ist damit der Betriebsrat nach dem Betriebsverfassungsgesetz am Zug, im öffentlichen Haus der Personalrat nach dem jeweiligen Landespersonalvertretungsgesetz, im kirchlichen Haus die Mitarbeitervertretung nach MAVO oder MVG. Eine Dienst- oder Betriebsvereinbarung, die Zweck, berechtigte Auswerter und Löschfristen festlegt, schafft Vertrauen. Und sie macht deutlich, dass es um den Schutz der Patienten geht, nicht um die Suche nach Schuldigen. Wer bei einem Richtlinientipp an Strafe denkt, weicht auf das private Handy aus.

Der Entscheidungsweg für den Alltag

Am Ende braucht die Station keine Rechtsgrundlagen, sondern eine Antwort auf die Frage: Darf das hier rein? Der folgende Entscheidungsweg gehört als Anhang in die Verfahrensanweisung, an die Pinnwand im Dienstzimmer und in die Wissensdatenbank der IT-Hotline.



Skizze: Der gelbe Kasten ist eine Ausnahme mit Ablaufdatum, kein Dauerzustand.

WICHTIG · Jede Ausnahme ist eine KIS-Anforderung

Führen Sie zu jeder freigegebenen Ausnahme eine Anforderung an den KIS-Hersteller oder die KIS-Abteilung mit. Die Liste der Ausnahmen ist zugleich die priorisierte Wunschliste für das nächste KIS-Release und ein gutes Argument in der Budgetbesprechung mit der Geschäftsführung.

Häufige Fragen

Dürfen Patientendaten grundsätzlich nie in Microsoft 365 liegen?

Der Grundsatz lautet: Behandlungsdokumentation gehört ins KIS. Ob es eng begrenzte Ausnahmen geben darf, entscheidet der Verantwortliche mit dem Datenschutzbeauftragten, unter Berücksichtigung von § 393 SGB V, Schweigepflicht, Landesrecht und Trägerrecht. Wenn ja, dann in geschützten Bereichen mit Bezeichnung, DLP, ohne Gäste und mit Löschfrist.

Reicht es nicht, Patientendaten in Teams einfach zu verbieten?

Ein Verbot ohne Alternative verlagert die Daten auf private Messenger und Privatgeräte. Wirksamer ist, die Ursache zu beheben, meistens eine fehlende KIS-Funktion, und den Rest mit Leitplanken sichtbar zu machen.

Erkennt Microsoft Purview deutsche Patientendaten von selbst?

Nur teilweise. Es gibt mitgelieferte Informationstypen für deutsche Ausweisdokumente und medizinische Begriffslisten, eine eingebaute Erkennung der Krankenversichertennummer ist in der Liste nicht enthalten. Eigene Informationstypen für Versicherten-, Fall- und Patientennummern des Hauses sind deshalb Pflicht.

Was ist mit anonymisierten oder pseudonymisierten Daten?

Echte Anonymisierung, bei der kein Rückschluss auf Personen möglich ist, macht Kennzahlen zu einem guten Fall für Microsoft 365. Pseudonymisierte Daten bleiben personenbezogen. Bei kleinen Fallzahlen, seltenen Erkrankungen oder Angaben zu Zimmer und Datum ist die Grenze schneller überschritten, als man denkt.

Sind Microsoft-365-Dienste durch ein C5-Testat abgedeckt?

Das müssen Sie für die konkret genutzten Dienste prüfen. Die aktuellen Berichte stellt Microsoft im Service Trust Portal bereit. Dokumentieren Sie, welcher Dienst von welchem Testat welchen Typs erfasst ist, und wiederholen Sie die Prüfung, wenn Testate erneuert werden.

Muss der Betriebsrat, Personalrat oder die MAV bei DLP beteiligt werden?

DLP-Berichte und Protokollauswertungen können Verhalten erfassen. Damit ist die Mitbestimmung in aller Regel berührt, je nach Trägerschaft nach unterschiedlichem Recht. Beziehen Sie die Interessenvertretung früh ein und regeln Sie Zweck und Auswertung in einer Vereinbarung.

Wo fange ich an, wenn die Grauzonen schon überall sind?

Mit einer Bestandsaufnahme: DLP im Simulationsmodus, Auswertung der Teams und Sites mit Gastzugriff, Gespräche mit Stationsleitungen. Danach die riskantesten Fälle zuerst, meist externe Mails und Gastkonten, und parallel die Liste der KIS-Anforderungen.

Fazit: Die Grenze ziehen, die Lücken schließen

Patientendaten und Microsoft 365 sind kein Liebespaar, aber sie begegnen sich täglich auf dem Flur. Die Grundregel bleibt einfach: Behandlungsdokumentation gehört ins KIS, Microsoft 365 trägt Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Die Grauzonen dazwischen verschwinden nicht durch Rundschreiben. Sie verschwinden, wenn das KIS die fehlende Funktion bekommt, wenn die Leitplanken in Microsoft 365 den falschen Weg unbequem machen und wenn eine Verfahrensanweisung klar sagt, was gilt.

Die Belegungsliste mit dem Namen „NICHT_LÖSCHEN“ darf am Ende übrigens tatsächlich gelöscht werden. Aber erst, wenn die Station etwas Besseres hat. Wenn Sie die Grenze für Ihr Haus oder Ihren Klinikverbund ziehen und die Leitplanken planen wollen, unterstützt Sie die Microsoft-365-Beratung für Krankenhäuser. Für Administratoren, Datenschutz und QM gibt es die passende Microsoft-365-Schulung für Krankenhäuser.

WEITERLESEN · Weiterlesen

Passende Kompetenzbereiche zu diesem Beitrag:

› Microsoft Purview
› SharePoint
› Microsoft Entra ID
› Microsoft 365 Security
› Microsoft 365 Copilot
› Dokumentenlenkung nach ISO 9001
› NIS2 technisch umsetzen mit Microsoft 365