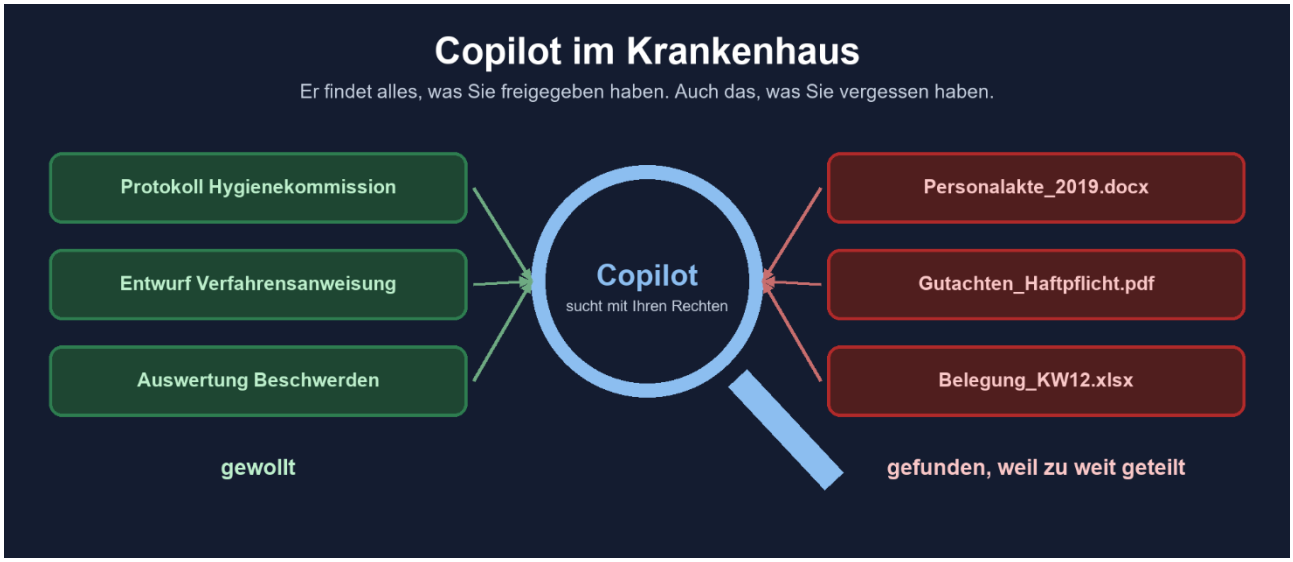
Copilot im Krankenhaus: Oversharing, Patientenbezug und die Frage, wer ihn überhaupt bekommt



Wissen

Der Überblick zur ganzen Serie: Recht, Technik und Organisation von Microsoft 365 in der Klinik.

› Microsoft 365 im Krankenhaus

Beratung

Copilot- und Oversharing-Überprüfung für Ihr Haus oder Ihren Klinikverbund, bevor die erste Lizenz zugewiesen ist.

› Microsoft-365-Beratung für Krankenhäuser

Schulung

Pilotgruppe, Site-Besitzer und Administratoren fit machen für Copilot, Freigaben und Kennzeichnung.

› Microsoft-365-Schulung für Krankenhäuser

Irgendwann kommt die Mail aus der Geschäftsführung. Meist nach einer Fachtagung, manchmal nach einem Gespräch mit dem Träger, gelegentlich nach einem Zeitungsartikel: „Wir sollten Copilot einführen. Was kostet das, und wann geht es los?“ Die ehrliche Antwort auf die zweite Frage lautet in den meisten Häusern: später, als Sie denken. Nicht wegen der Technik, nicht wegen des Geldes, sondern wegen dessen, was Copilot in Ihrem Tenant finden wird, sobald Sie ihn lassen.

Microsoft 365 Copilot ist im Krankenhaus kein exotisches Werkzeug mehr. Die Grundstufe, der Copilot Chat, steckt in den gängigen Plänen ohne Aufpreis drin und ist bei vielen Häusern längst sichtbar, ob jemand das beschlossen hat oder nicht. Die volle Copilot-Lizenz dagegen arbeitet mit allem, worauf das angemeldete Konto zugreifen darf: Postfach, Chats, Besprechungen, OneDrive, SharePoint, Teams. Und damit mit zehn Jahren Freigabepraxis eines Hauses, in dem „Mach das mal für alle sichtbar, dann findet es jeder“ lange als Lösung galt.

Dieser Beitrag richtet sich an IT-Leitungen, Geschäftsführungen, Informationssicherheits- und Datenschutzbeauftragte, Qualitätsmanagement und die Interessenvertretung in Akutkrankenhäusern, Fach- und Rehakliniken, Universitätsklinika und Klinikverbünden. Er klärt, was Copilot Chat und die Copilot-Lizenz unterscheidet, warum Oversharing das eigentliche Risiko ist, in welcher Reihenfolge Sie vorgehen sollten und welche Personengruppen zuerst sinnvoll sind. Medizinische Einsatzfelder, also alles rund um Diagnostik, Therapie und Befundung, klammern wir bewusst aus: Dort gelten Medizinprodukterecht und Haftungsfragen, die ein eigenes Thema

sind. Arztpraxen, Pflegeheime und Krankenkassen haben andere Rahmenbedingungen und sind hier nicht gemeint.

Fakten: Das Wichtigste in Kürze

- Microsoft hat umbenannt: Aus „Microsoft 365 Copilot“ wurde in der Dokumentation „Microsoft Copilot“, aus „Microsoft 365 Copilot Chat“ wurde „Microsoft Copilot Chat“. Gemeint ist dasselbe.
- Copilot Chat steht laut Microsoft ohne Zusatzkosten bereit, wenn sich jemand mit dem Entra-Konto anmeldet und einen berechtigten Plan hat, darunter Microsoft 365 E3, E5, F1 und F3 sowie Office 365 E1, E3, E5 und F3.
- Die Copilot-Lizenz ist eine Ergänzung. Microsoft listet als Voraussetzung unter anderem Microsoft 365 E3, E5, F1 und F3; Microsoft 365 E7 enthält Copilot bereits.
- Copilot zeigt nur, was das Konto ohnehin sehen darf. Genau das ist das Problem, wenn diese Rechte seit Jahren zu weit gefasst sind.
- Reihenfolge: Berechtigungslage prüfen, sensible Bestände ausschließen bzw. kennzeichnen, pilotieren, ausrollen. Die Vertretung sitzt von Anfang an mit am Tisch.

Was es gibt und wer es bekommt: Copilot Chat und die Copilot-Lizenz

Bevor Sie über Personengruppen reden, lohnt ein Blick auf die zwei Stufen, die Microsoft anbietet. Sie unterscheiden sich nicht nur im Preis, sondern vor allem darin, was Copilot sehen kann. Und das ist im Krankenhaus die Frage, an der alles hängt.

Copilot Chat: schon im Haus, ob beschlossen oder nicht

Copilot Chat ist die Grundstufe. Laut Microsoft ist er für Personen mit Entra-Konto und berechtigtem Plan ohne Zusatzkosten verfügbar. Für Krankenhäuser relevant sind vor allem Microsoft 365 E3, E5 und E7, die Frontline-Pläne F1 und F3, Office 365 E1, E3, E5 und F3 sowie die Business-Pläne, die kleinere Fach- und Rehakliniken nutzen. Auch die Varianten ohne Teams und die EWR-Varianten sind eingeschlossen. Welche Pläne Ihr Haus konkret hat und wie sie sich verteilen, behandelt der Beitrag Lizenzen im Krankenhaus: Frontline für die Pflege, Vollausstattung für die Verwaltung.

Copilot Chat arbeitet mit dem Web, mit Dateien, die jemand hochlädt, und mit dem Dokument, das gerade in Word, Excel oder PowerPoint geöffnet ist. Er durchsucht nicht von sich aus Postfächer, Teams oder SharePoint-Sites. Die Gefahr liegt hier woanders: Wer eine Excel-Liste mit Patientennamen öffnet und um eine Zusammenfassung bittet, hat Copilot Chat diese Liste gerade selbst gegeben. Das ist kein Oversharing im technischen Sinne, sondern ein Regelungs- und Schulungsthema.

Für die Planung wichtig: Copilot Chat ist für die meisten berechtigten Personen standardmäßig angeheftet. Das Lösen dieser Anheftung entfernt den Zugang nicht, Copilot Chat bleibt über die Copilot-App erreichbar. Für Mandanten mit Hauptstandort im EWR oder in der Schweiz steuert die Anheft-Einstellung die Copilot-App seit dem 25. Juli 2025 ohnehin nicht mehr. Wer Copilot Chat für bestimmte Gruppen wirklich nicht will, sperrt den Zugriff im Microsoft 365 Admin Center, laut Dokumentation für alle oder gezielt für Benutzer und Gruppen, und kann eine eigene Seite mit der Hausregel hinterlegen, die beim Sperrhinweis erscheint.

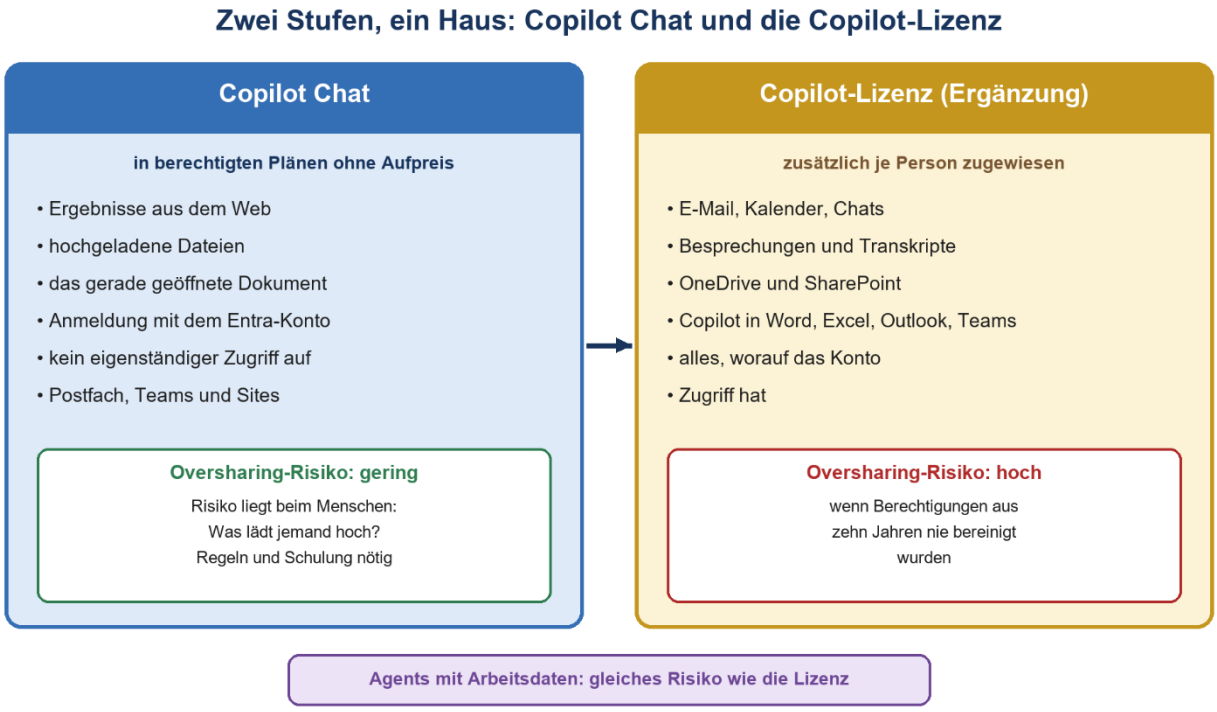
Die Copilot-Lizenz: Zugriff auf alles, was das Konto sehen darf

Erst mit der Copilot-Lizenz arbeitet Copilot mit den Arbeitsdaten im Tenant: E-Mail, Kalender, Chats, Besprechungen und Transkripte, OneDrive, SharePoint und Teams, und er ist voll in Word, Excel, PowerPoint, Outlook und Teams integriert. Microsoft beschreibt das so, dass Copilot nur auf Daten zugreift, für die die Person berechtigt ist, und bestehende Berechtigungen, Freigabeeinstellungen und Richtlinien respektiert. Das klingt beruhigend und ist korrekt. Es ist nur kein Trost, wenn diese Berechtigungen das Problem sind.

Die Liste der Voraussetzungen steht unter Lizenzoptionen für Microsoft Copilot bei Microsoft Learn. Für Krankenhäuser genügt die Kurzfassung: Die Lizenz lässt sich auf die gängigen Enterprise- und Frontline-Pläne aufsetzen, Microsoft 365 E7 enthält sie bereits. Preise nennen wir bewusst nicht, sie ändern sich schneller als die Dienstplanung im Dezember.

Agents: die Grauzone dazwischen

Zwischen den beiden Stufen liegen Agents. Auch Personen ohne Copilot-Lizenz können Agents nutzen, die auf Arbeitsdaten zugreifen, etwa auf eine bestimmte SharePoint-Site. Für die Berechtigungsfrage macht das keinen Unterschied: Ein Agent, der auf eine zu weit geteilte Site zeigt, findet dort genau dasselbe wie der lizenzierte Copilot. Wer Agents zulässt, braucht dieselbe Vorarbeit wie für die Lizenz.



Skizze 1: Copilot Chat arbeitet mit dem, was jemand ihm gibt. Die Copilot-Lizenz arbeitet mit allem, was das Konto darf.

Merkmal	Copilot Chat	Copilot-Lizenz (Ergänzung)
Kosten	in berechtigten Plänen ohne Aufpreis	zusätzliche Lizenz je Person
Datengrundlage	Web, hochgeladene und geöffnete Dateien	alles, worauf das Konto im Tenant Zugriff hat
Office-Apps	Chat mit Bezug auf das offene Dokument	voll integriert in Word, Excel, PowerPoint, Outlook, Teams

Merkmal	Copilot Chat	Copilot-Lizenz (Ergänzung)
Besprechungen	kein Zugriff auf Transkripte im Tenant	Zusammenfassungen, Aufgaben, Transkripte
SharePoint Advanced Management	nicht automatisch	Copilot-bezogene Funktionen, sobald eine Lizenz zugewiesen ist
Oversharing-Risiko	gering, solange keine Agents auf Sites zeigen	hoch, wenn Berechtigungen nicht bereinigt sind
Typischer Fehler	Patientenliste selbst hochladen	Lizenz vor der Bereinigung zuweisen

Wichtig: Lizenzstand vor jeder Bestellung prüfen

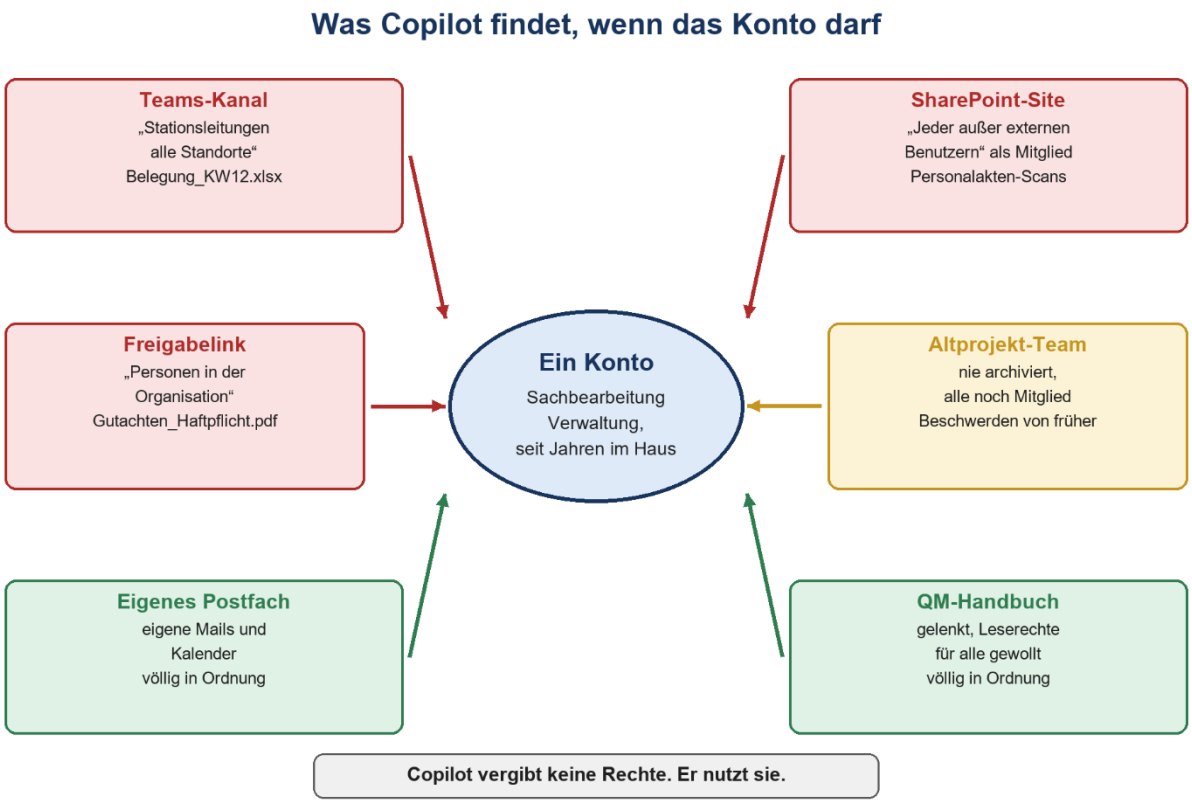
Microsoft ändert Namen, Bündel und Voraussetzungen in kurzen Abständen. Die Angaben in diesem Beitrag entsprechen der Dokumentation bei Microsoft Learn zum Stand Oktober 2026. Prüfen Sie vor jeder Bestellung die aktuelle Liste der Voraussetzungen und lassen Sie sich die Zuordnung zu Ihrem Vertrag schriftlich bestätigen.

Das eigentliche Risiko: Oversharing aus zehn Jahren Zusammenarbeit

Die meisten Diskussionen über Copilot im Krankenhaus drehen sich um die falsche Frage. „Was macht Microsoft mit unseren Daten?“ ist wichtig und wird in den Abschnitten zu Datenschutz und Testaten behandelt. Die Frage, die Ihnen im Pilotbetrieb tatsächlich um die Ohren fliegt, ist eine andere: „Was darf eigentlich die Sachbearbeitung im Einkauf alles lesen?“ Denn die Antwort war schon vor Copilot dieselbe. Nur hat sie bisher niemand gesucht.

Copilot vergibt keine Rechte, er nutzt sie

Copilot hebelt keine Berechtigungen aus. Er macht etwas viel Unangenehmeres: Er macht vorhandene Berechtigungen nutzbar. Bisher schützte im Krankenhaus oft die Unauffindbarkeit. Die Personalakte lag in einer Site, deren Namen niemand kannte. Das Gutachten zur Haftpflichtsache hing an einem Freigabelink, den nur drei Leute hatten, der aber für „Personen in der Organisation“ galt. Die Beschwerde-Ablage stammte aus einem Projekt, dessen Team nie archiviert wurde. Mit einer Frage wie „Fasse mir alles zusammen, was es zu Station 4 gibt“ ist diese Art Schutz Geschichte.



Skizze 2: Ein ganz normales Konto, ganz normale Rechte und ein paar Altlasten. Copilot findet alles davon.

Was sich in Klinik-Tenants typischerweise findet

Die folgende Übersicht ist kein Vorwurf, sondern Erfahrung: Diese Bestände entstehen, weil Menschen unter Druck pragmatisch arbeiten. Sie gehören trotzdem vor dem Piloten auf den Tisch.

Bestand	Typischer Ort	Warum heikel	Erste Maßnahme
Personalakten, Abmahnungen, BEM-Unterlagen	Site der Personalabteilung mit vererbten Rechten, Scans in OneDrive	Daten von Mitarbeiterinnen und Mitarbeitern, teils Gesundheitsdaten	Zugriff an Gruppe binden, Freigabelinks entfernen
Gutachten, Haftpflicht- und Rechtsfälle	Postfach-Anhänge, die in Teams abgelegt wurden; Links an Externe	Rechtlich sensibel, oft mit Patientenbezug	Ablage klären, Vertraulichkeitsbezeichnung, Auffinden sperren
Beschwerden und Patientenfürsprache	Altprojekt-Team, Excel-Liste im Kanal	Namen, Vorgänge, Bewertungen von Personen	Prüfen, ob die Ablage ins Beschwerdemanagement gehört
Belegungslisten mit Patientennamen	Teams-Kanal der Stationsleitungen, OneDrive-Freigabe	Patientendaten außerhalb des KIS, Schweigepflicht	Klären, zurück ins KIS, Zugriff sofort schließen
Dienstpläne mit Krankmeldungen	Excel in SharePoint, oft für die ganze Abteilung	Gesundheitsdaten der Belegschaft	Inhalte trennen, Rechte auf die Dienstplanung beschränken
Gehaltslisten, Vertragsentwürfe Chefärzte	OneDrive der Geschäftsführung, geteilt per Link	Vertraulich, arbeitsrechtlich sensibel	Links prüfen, Ablaufdatum, Bezeichnung

Bestand	Typischer Ort	Warum heikel	Erste Maßnahme
Unterlagen von Aufsichtsrat und Träger	Gremien-Team mit vielen Gästen	Strategisch, teils nicht öffentlich	Mitgliedschaften prüfen, Gäste befristen
Sicherheitsvorfälle, Forensik	IT-Site, Ticketsystem-Exporte	Angreifer-Wissen, Kontonamen, Schwachstellen	Eng begrenzen, Auffinden sperren

Patientenbezug: die Excel-Liste, die es nicht geben sollte

Die Grundhaltung dieser Serie ist eindeutig: Patientendaten gehören ins KIS und seine Subsysteme, also LIS, RIS, PACS und was ein Haus sonst an Fachverfahren betreibt. Microsoft 365 ist Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Wo das KIS endet und das Office anfängt, behandelt der Beitrag Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt ausführlich.

Die Realität sieht in vielen Häusern trotzdem so aus, dass irgendwo eine Belegungsliste, eine OP-Planung als Excel oder eine Übergabeliste in einem Teams-Kanal liegt. Meist aus einem nachvollziehbaren Grund, etwa weil das KIS an einer Stelle umständlich ist oder weil es in einer Ausnahmelage schnell gehen musste. Das ist verständlich und trotzdem nicht der Normalfall, den man mit Copilot zementieren sollte. Welche Kanäle in Teams nichts zu suchen haben, steht im Beitrag Teams im Krankenhaus: Gremien, Projekte, Kommissionen und wo Teams nichts zu suchen hat.

Warnung: Copilot macht Patientenlisten auffindbar, nicht zulässig

Copilot ändert nichts an der Rechtslage einer Patientenliste in Teams. Er ändert, wie leicht sie gefunden wird. Ein Haus, das Copilot lizenziert, bevor solche Bestände geklärt sind, verwandelt ein verstecktes Problem in ein sichtbares. Das kann man als Chance sehen. Besser ist, es vorher selbst zu sehen.

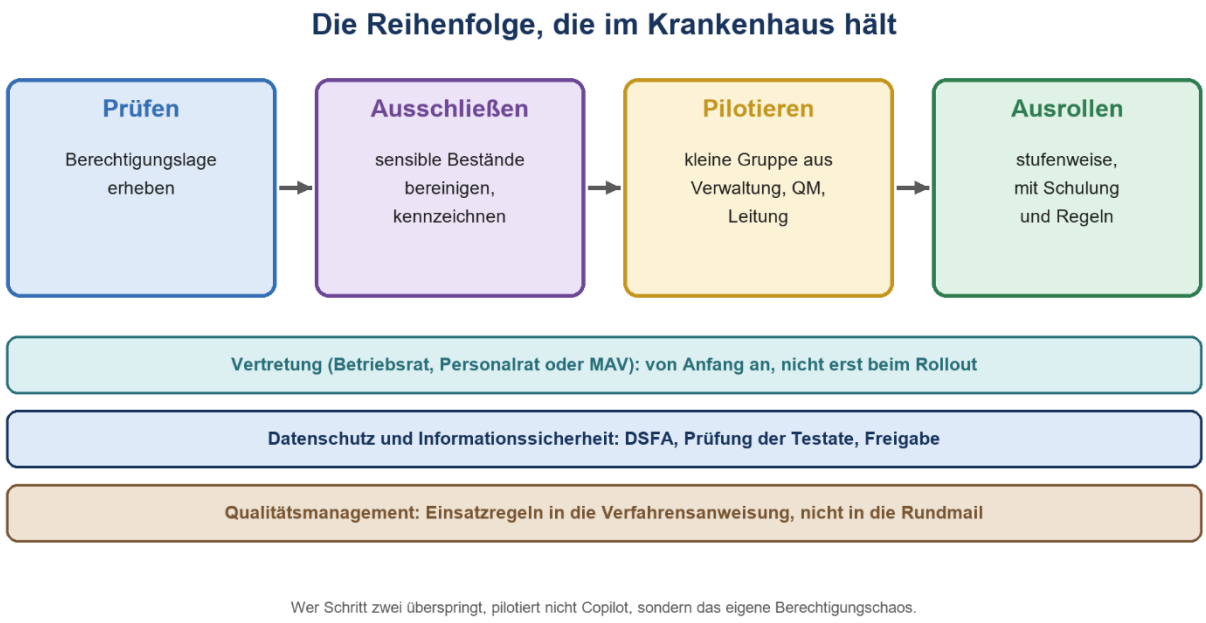
Zur Schweigepflicht, zu § 203 StGB und den Landeskrankenhausgesetzen lesen Sie Schweigepflicht und Cloud: § 203 StGB, Landeskrankenhausgesetze und Auftragsverarbeitung.

Aus der Praxis: Worauf das Konto Zugriff hatte

Aus der langjährigen Begleitung eines Krankenhausverbunds mit mehreren Standorten, unter anderem bei Vertrauensstellungen, PKI und forensischen Untersuchungen: Die Frage „Worauf hatte dieses Konto eigentlich Zugriff?“ ist immer schneller gestellt als beantwortet. Copilot stellt diese Frage jeden Tag, für jedes lizenzierte Konto, und beantwortet sie sofort. Wer sie vorher selbst beantwortet hat, schläft ruhiger.

Die Reihenfolge: prüfen, ausschließen, pilotieren, ausrollen

Für Copilot im Krankenhaus gibt es eine Reihenfolge, die hält, und viele, die im Pilotbetrieb scheitern. Die haltbare sieht so aus: erst die Berechtigungslage prüfen, dann sensible Bestände ausschließen bzw. kennzeichnen, dann mit einer kleinen Gruppe pilotieren und erst danach ausrollen. Begleitend laufen Datenschutz, Informationssicherheit, Qualitätsmanagement und die Interessenvertretung mit.



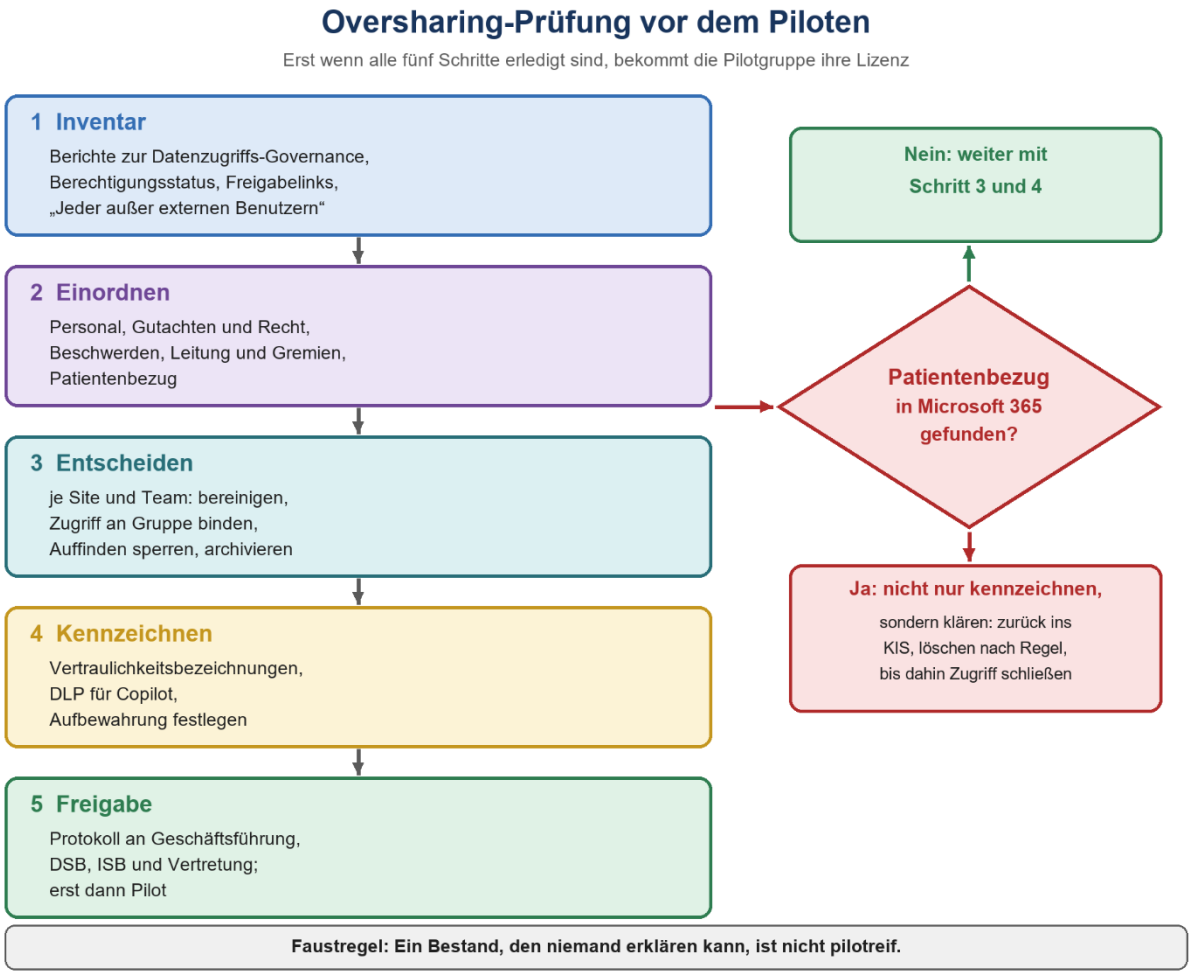
Skizze 3: Vier Phasen, drei Begleitbahnen. Keine davon ist optional.

Schritt 1: Berechtigungslage prüfen

Die Werkzeuge dafür liefert Microsoft inzwischen selbst. SharePoint Advanced Management, kurz SAM, enthält das Content Management Assessment, das überteilte Inhalte, besitzerlose und inaktive Sites aufspürt und Empfehlungen gibt. Microsoft rät, die Bewertung alle 30 Tage zu wiederholen. Dazu kommen die Berichte zur Datenzugriffs-Governance: der Bericht zum Berechtigungsstatus über alle SharePoint- und OneDrive-Sites, der Bericht, welche Sites eine bestimmte Person erreicht, die Auswertung der Freigabe an „Jeder außer externen Benutzern“ und die Berichte zu Freigabelinks der letzten 28 Tage. Aus diesen Berichten heraus lassen sich Site-Zugriffsüberprüfungen an die Site-Besitzer delegieren.

Ein lizenzrechtliches Detail, das oft übersehen wird: Laut Microsoft erhalten SharePoint-Administratoren die Copilot-bezogenen SAM-Funktionen automatisch, sobald im Tenant mindestens einer Person eine Copilot-Lizenz zugewiesen ist. Ein einzelnes Konto in der IT reicht also, um die Prüfwerkzeuge freizuschalten, ohne dass die Belegschaft schon Copilot hat. Einige Funktionen setzen dagegen das eigenständige SAM-Add-on voraus.

Ergänzend bietet Microsoft Purview mit dem Data Security Posture Management Datenrisikobewertungen, die überteilte Sites mit sensiblen Inhalten und riskanten Freigabelinks zeigen. Im Microsoft 365 Admin Center gibt es zudem ein Copilot-Sicherheits-Dashboard für Datenschutz, Oversharing und Compliance. Auf Seite der Identitäten gehören Gastkonten, verwaiste Gruppen und Altkonten in die Prüfung; mehr dazu im Kompetenzbereich Microsoft Entra ID.



Skizze 4: Die Oversharing-Prüfung vor dem Piloten. Patientenbezug ist kein Kennzeichnungsfall, sondern ein Klärungsfall.

Schritt 2: Sensible Bestände ausschließen bzw. kennzeichnen

Aus der Inventur folgt für jeden auffälligen Bestand eine Entscheidung. Die Werkzeuge unterscheiden sich darin, ob sie das Problem lösen oder nur verdecken. Das sollten Sie in der Entscheidungsvorlage für die Geschäftsführung sauber auseinanderhalten.

Werkzeug	Was es bewirkt	Grenze
Berechtigungen bereinigen	Zugriff entspricht wieder dem Bedarf	Aufwand, braucht Site-Besitzer, die mitmachen
Restricted Access Control	Zugriff auf eine Site an eine Entra- oder Microsoft-365-Gruppe binden, unabhängig von Einzelfreigaben	Gruppe muss gepflegt werden
Restricted Content Discovery	Site taucht nicht mehr in Copilot, Agents und organisationsweiter Suche auf	Berechtigungen bleiben unverändert; wer den Weg kennt, kommt weiter hin
Vertraulichkeitsbezeichnungen	Kennzeichnung und Schutz auf Datei-, Site- und Team-Ebene	Wirkt nur, wenn konsequent vergeben
DLP für Copilot	Copilot und Agents fassen Inhalte mit bestimmten Bezeichnungen nicht zusammen	Setzt Bezeichnungen voraus, Lizenzlage prüfen
Microsoft 365 Archive	Inaktive Sites ins Archiv; dort für	Archivieren ist kein Löschen,

Werkzeug	Was es bewirkt	Grenze
	Benutzer und Copilot nicht erreichbar	Fristen gelten weiter
Aufbewahrung und Löschung	Alte Bestände regelgerecht beenden	Nur für Verwaltungsunterlagen, nicht für die Patientenakte

Für die Fristenfrage verweisen wir auf Aufbewahrung im Krankenhaus mit Purview: Fristen für Verwaltungsunterlagen, nicht für die Patientenakte. Ein gelenktes QM-Handbuch ist übrigens das Gegenbeispiel zu allem oben: klare Leserechte für alle, klare Bearbeitungsrechte für wenige, gültige und ungültige Fassungen sauber getrennt. Für Copilot ist das ideal, wie der Beitrag QM-Handbuch mit SharePoint: Dokumentenlenkung im Krankenhaus, die im Audit hält zeigt.

Tipp: Restricted Content Discovery ist ein Vorhang, kein Schloss

Restricted Content Discovery ist hervorragend, um heikle Sites für den Piloten schnell aus der Copilot-Suche zu nehmen. Microsoft betont selbst, dass die Berechtigungen dabei unverändert bleiben. Setzen Sie es als Überbrückung mit Enddatum ein und hinterlegen Sie in der Maßnahmenliste, wer bis wann die eigentliche Bereinigung erledigt.

Schritt 3: Pilotieren

Der Pilot ist kein Showcase für die Geschäftsführung, sondern ein Test unter realen Bedingungen. Bewährt hat sich eine kleine Gruppe aus Qualitätsmanagement, Controlling, Assistenz der Geschäftsführung, Gremienarbeit und IT, ergänzt um eine Person aus der Personalabteilung, sobald deren Bestände bereinigt sind. Legen Sie vorher fest, welche Aufgaben getestet werden, wie Rückmeldungen gesammelt werden und was ein Abbruchkriterium ist, etwa ein Fund mit Patientenbezug, der nicht in der Inventur stand.

- **Fundmeldung:** Wer im Piloten etwas findet, das er nicht sehen sollte, meldet es über einen festen Weg, ohne dass daraus ein Vorwurf wird. Diese Meldungen sind der wertvollste Ertrag des Piloten.
- **Aufgabenkatalog:** Protokoll aus der Kommissionssitzung, Entwurf einer Verfahrensanweisung, Auswertung einer Excel-Tabelle, Zusammenfassung eines langen Mailverlaufs.
- **Auswertung:** Nutzungsberichte dienen der Steuerung des Piloten, nicht der Bewertung einzelner Personen. Das gehört schriftlich in die Vereinbarung mit der Vertretung.
- **Dauer:** Lang genug, dass der Neuheitseffekt verfliegt, kurz genug, dass Ergebnisse vor der nächsten Budgetrunde vorliegen.

Schritt 4: Ausrollen

Ausgerollt wird stufenweise und an Gruppen gebunden, nicht an Begeisterung. Jede neue Gruppe bringt eigene Bestände mit, die Sie vorher mit denselben Berichten prüfen. Parallel gehören Einsatzregeln ins QM-System: als Verfahrensanweisung mit Geltungsbereich, Verantwortlichen und Freigabe, nicht als Rundmail, die in drei Wochen vergessen ist. Schulungen für Pilotgruppe, Site-Besitzer und Administratoren bietet die Microsoft-365-Schulung für Krankenhäuser.

Tipp: Copilot- und Oversharing-Überprüfung für Ihr Haus

Sie wollen wissen, was Copilot in Ihrem Tenant finden würde, bevor es die Pilotgruppe tut? In der Copilot- und Oversharing-Überprüfung werten wir die Berechtigungslage aus, ordnen die

Funde mit Ihnen ein und liefern eine Maßnahmenliste samt Vorlage für die Geschäftsführung.

› Microsoft-365-Beratung für Krankenhäuser

› Microsoft 365 Copilot

Wer ihn bekommt: Personengruppen, Einsatzfelder und Grenzen

Die Frage „Wer bekommt Copilot?“ beantwortet sich im Krankenhaus nicht nach Hierarchie, sondern nach zwei Kriterien: Wie viel Nutzen hat die Person im Alltag, und wie groß ist das Risiko, dass ihr Konto Dinge findet, die es nicht finden sollte? Beides ist je Haus verschieden, aber die Muster ähneln sich.

Sinnvolle Einsatzfelder in Verwaltung, QM und Leitung

- **Protokolle:** Zusammenfassungen und Aufgabenlisten aus Kommissions-, Projekt- und Leitungsrunden. Ob Besprechungen dafür aufgezeichnet oder transkribiert werden, ist eine Regelungsfrage mit der Vertretung.
- **Entwürfe von Verfahrensanweisungen:** Gliederung, Formulierung, Abgleich mit bestehenden Dokumenten. Freigabe bleibt bei den Verantwortlichen im gelenkten Verfahren.
- **Auswertungen:** Excel-Auswertungen aus Controlling, Einkauf oder aggregierten Kennzahlen, Erklärungen zu Formeln, Diagramme für die Vorlage.
- **Korrespondenz und Vorlagen:** Antworten auf Anfragen, Gremienvorlagen, Zusammenfassung langer Mailverläufe, Vorbereitung von Ausschreibungen.
- **Recherche im eigenen Bestand:** „Was haben wir zur Hygienekommission im letzten Jahr beschlossen?“ Funktioniert, wenn die Ablage ordentlich ist, und zeigt gnadenlos, wenn nicht.

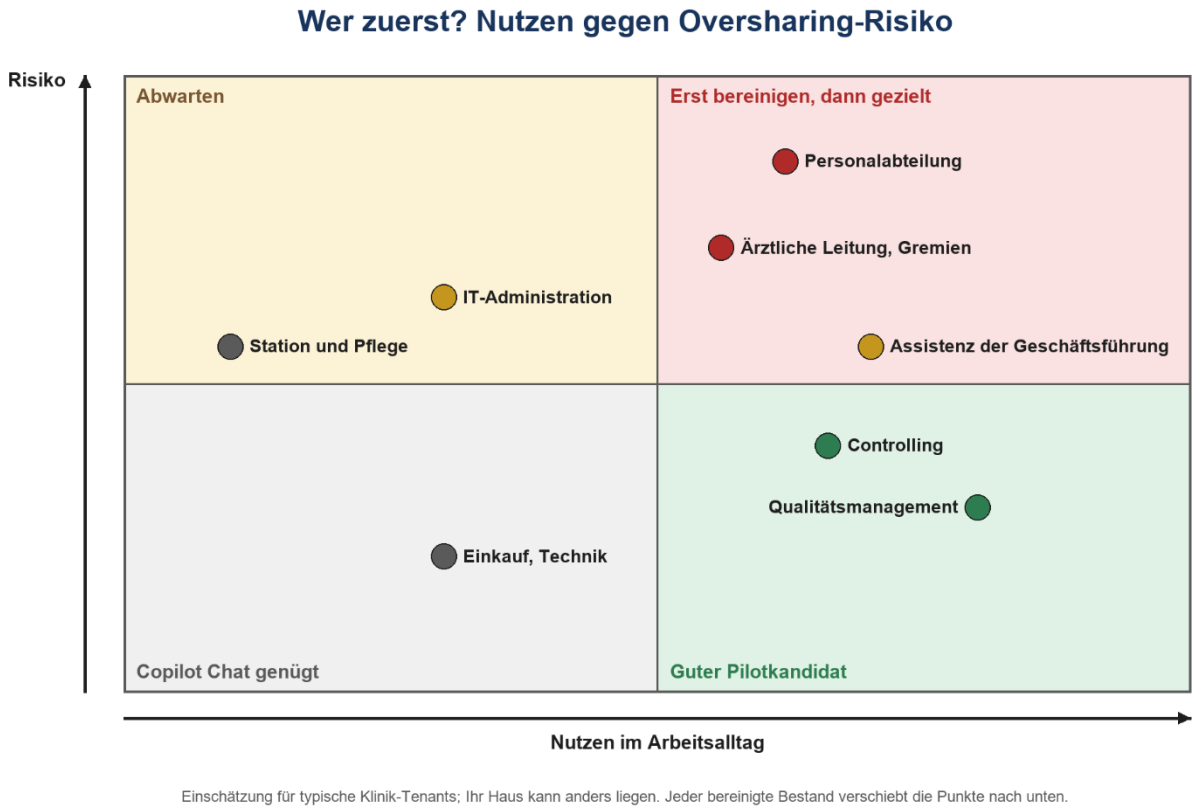
Warnung: Medizinische Einsatzfelder sind nicht Thema dieses Beitrags

Diagnostik, Therapie, Befundung, Arztbriefe und alles, was in die Behandlung von Patienten eingreift, klammern wir ausdrücklich aus. Dort stellen sich Fragen des Medizinprodukterechts und der Haftung, die eine eigene Bewertung brauchen. Ein Verwaltungswerkzeug wird nicht dadurch zum geeigneten Werkzeug für die Station, dass es auch dort installiert ist. Legen Sie das in den Einsatzregeln ausdrücklich fest.

Personengruppen im Überblick

Personengruppe	Nutzen	Risiko	Empfehlung
Qualitätsmanagement (QMB)	hoch: Verfahrensanweisungen, Auditvorbereitung, Protokolle	gering bis mittel, wenn das QM-Handbuch gelenkt ist	Pilotkandidat der ersten Welle
Controlling, kaufmännische Verwaltung	hoch: Auswertungen, Berichte, Vorlagen	mittel: Zugriff auf Finanz- und Leistungsdaten	Pilot, nach Prüfung der Finanz-Sites
Geschäftsführung und Assistenz	hoch: Mailflut, Vorlagen, Gremien	mittel bis hoch: Zugriff auf fast alles	Pilot nach Bereinigung der Gremien- und Vertragsablagen
Personalabteilung	mittel bis hoch: Schreiben,	hoch: Personalakten, BEM, Gesundheitsdaten	Erst nach eigener Bereinigung; keine

Personengruppe	Nutzen	Risiko	Empfehlung
	Auswertungen	der Belegschaft	Nutzung für Personalauswahl oder Leistungsbewertung
Ärztlicher Direktor, Pflegedirektion, Chefärzte	mittel: Gremien, Korrespondenz, Organisation	hoch: Gutachten, Beschwerden, Fälle mit Patientenbezug	Später, nur für Organisationsaufgaben
IT-Administration	mittel: Skripte, Dokumentation, Analyse	mittel: weitreichende Rechte, Sicherheitsunterlagen	Ein Konto früh für Prüfwerkzeuge; Admin-Konten ohne Copilot
Station und Pflege	gering im Copilot-Sinn: Arbeit findet im KIS statt	mittel: Kanäle mit Übergaben, gemeinsam genutzte Geräte	Keine Copilot-Lizenz; Copilot Chat nur mit klaren Regeln
Medizintechnik	mittel: Dokumentation, Herstellerkorrespondenz	gering bis mittel	Später; Gerätedokumentation bleibt im CAFM bzw. gelenkt



Skizze 5: Nutzen gegen Risiko. Ein Startvorschlag, kein Naturgesetz.

Station und Pflege: lizenzrechtlich möglich heißt nicht sinnvoll

Microsoft listet F1 und F3 als Voraussetzung für die Copilot-Lizenz, und Copilot Chat ist in diesen Plänen enthalten. Lizenzrechtlich ginge also einiges. Fachlich ist die Station selten der richtige Einstieg: Die eigentliche Arbeit findet im KIS statt, Stationsrechner werden im Schichtdienst gemeinsam genutzt, und die Kanäle, in denen Pflegekräfte sich organisieren, enthalten häufiger als anderswo Bezüge zu Patienten. Wie gemeinsam genutzte Geräte und Schichtwechsel sauber funktionieren, steht in Frontline in der Pflege: Gemeinsam genutzte Geräte, Schichtwechsel und

Stationsrechner. Für Copilot gilt dort: erst Regeln und Schulung, dann über Copilot Chat entscheiden, die Copilot-Lizenz vorerst gar nicht.

Recht und Mitbestimmung: AI Act, Datenschutz und die Vertretung

Wichtig: Keine Rechtsberatung

Die folgenden Hinweise ordnen ein, sie ersetzen keine rechtliche Prüfung. Landeskrankenhausgesetze, Landesdatenschutzgesetze und Personalvertretungsrecht unterscheiden sich je Bundesland, kirchliche Träger haben eigenes Datenschutz- und Mitarbeitervertretungsrecht. Beziehen Sie Ihren Datenschutzbeauftragten und, wo nötig, rechtliche Beratung ein.

EU AI Act: KI-Kompetenz und die Personalabteilung

Die KI-Verordnung der EU, Verordnung (EU) 2024/1689, ist in Kraft. Seit dem 2. Februar 2025 gelten die Verbote bestimmter Praktiken nach Artikel 5 und die Pflicht zur KI-Kompetenz nach Artikel 4: Betreiber von KI-Systemen sollen sicherstellen, dass ihr Personal über ausreichende Kenntnisse im Umgang verfügt. Für ein Krankenhaus, das Copilot einführt, heißt das praktisch: Schulung ist nicht nett, sondern Pflicht, und sie sollte dokumentiert sein, am besten im QM-System.

Ein zweiter Punkt betrifft die Personalabteilung. Anhang III der Verordnung zählt unter Beschäftigung KI-Systeme zu den Hochrisiko-Anwendungen, die für Auswahl von Bewerbern, Entscheidungen über Beförderung oder Kündigung sowie zur Leistungsbewertung eingesetzt werden. Copilot als Schreibhilfe ist kein solches System. Wer ihn aber Bewerbungen sortieren oder Mitarbeiterinnen und Mitarbeiter bewerten lässt, bewegt sich in genau diesem Feld. Schließen Sie solche Nutzungen in den Einsatzregeln aus. Die Fristen für die Hochrisiko-Pflichten waren zuletzt Gegenstand politischer Anpassungen; prüfen Sie den aktuellen Stand vor dem Zitieren.

Datenschutz, Testate und Landesrecht

Für Copilot und Copilot Chat beschreibt Microsoft einen Unternehmensdatenschutz auf Grundlage der Produktbedingungen und des Data Protection Addendum. Das ist die vertragliche Grundlage, ersetzt aber nicht die Bewertung im Haus: Ob eine Datenschutz-Folgenabschätzung nötig ist, entscheidet Ihr Haus mit dem Datenschutzbeauftragten; bei einem Werkzeug, das auf Personal- und Kommunikationsdaten zugreift, liegt sie nahe.

Für Sozial- und Gesundheitsdaten in Cloud-Diensten verlangt § 393 SGB V seit dem 1. Juli 2025 ein aktuelles C5-Testat vom Typ 2 oder ein gleichwertiges Testat bzw. Zertifikat nach der Verordnung. Ob und welche Copilot-Komponenten von welchem Testat abgedeckt sind, ist ein Prüfauftrag an Ihr Haus: Gleichen Sie den Geltungsbereich der Testate im Service Trust Portal mit den Diensten ab, die Sie nutzen. Einzelheiten stehen in § 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen. Die Sicherheitspflichten aus § 391 SGB V bzw. für Betreiber kritischer Anlagen aus dem BSIG und der B3S „Medizinische Versorgung“ der DKG in Version 1.3.1 gelten für Copilot wie für jeden anderen Dienst; sie verlangen vor allem, dass Sie wissen, wer worauf zugreift. Das ist dieselbe Arbeit wie die Oversharing-Prüfung, nur mit anderem Aktendeckel.

Vertretung einbinden: Betriebsrat, Personalrat oder MAV

Copilot verarbeitet Kommunikation, Besprechungen und Dokumente von Mitarbeiterinnen und Mitarbeitern und erzeugt Nutzungsdaten. Damit ist er eine technische Einrichtung, die zur Überwachung von Verhalten oder Leistung geeignet ist. In privaten Häusern greift § 87 Abs. 1 Nr. 6

BetrVG, in öffentlichen das Personalvertretungsrecht von Bund oder Land mit je eigenen Regeln, in kirchlichen Häusern die MAVO oder das MVG-EKD. Wer welches Recht hat und wie die Verfahren laufen, behandelt Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

Praktisch heißt das: Die Vertretung gehört in den Kreis, der die Oversharing-Prüfung auswertet und den Piloten zuschneidet, nicht erst in die Sitzung, in der der Rollout beschlossen werden soll. Bewährte Regelungspunkte einer Vereinbarung:

- Zweck und Geltungsbereich, ausdrücklich ohne medizinische Einsatzfelder
- Ausschluss von Leistungs- und Verhaltenskontrolle aus Copilot-Nutzungsdaten und Interaktionsverläufen
- Regeln für Aufzeichnung und Transkription von Besprechungen
- Keine Nutzung für Personalauswahl, Beförderung oder Bewertung
- Schulungsanspruch und Ansprechpartner
- Verfahren bei Funden im Piloten, ohne Schuldzuweisung
- Überprüfung nach einem festgelegten Zeitraum

FAQ: Copilot im Krankenhaus

Ist Copilot Chat in unserem Krankenhaus schon aktiv?

Wahrscheinlich ja. Copilot Chat ist für berechtigte Pläne wie Microsoft 365 E3, E5, F1 und F3 ohne Zusatzkosten verfügbar und meist standardmäßig angeheftet. Ob Sie ihn erlauben, einschränken oder für Gruppen sperren, entscheiden Sie im Microsoft 365 Admin Center.

Kann Copilot Chat ohne Lizenz unsere SharePoint-Sites durchsuchen?

Nicht von sich aus. Copilot Chat arbeitet mit Web, hochgeladenen und geöffneten Dateien. Der Zugriff auf Arbeitsdaten im Tenant setzt die Copilot-Lizenz voraus, oder einen Agent, der auf bestimmte Daten zeigt.

Umgeht Copilot unsere Berechtigungen?

Nein. Copilot zeigt nur, was das angemeldete Konto ohnehin sehen darf. Das Risiko entsteht, wenn diese Rechte über Jahre zu weit gefasst wurden, etwa durch „Jeder außer externen Benutzern“ oder Links für die ganze Organisation.

Reicht es, heikle Sites mit Restricted Content Discovery auszublenden?

Als Überbrückung ja, als Lösung nein. Die Site taucht dann nicht mehr in Copilot und der organisationsweiten Suche auf, die Berechtigungen bleiben aber unverändert. Die eigentliche Bereinigung muss folgen.

Brauchen wir für die Oversharing-Prüfung schon Copilot-Lizenzen?

Eine einzige reicht. Laut Microsoft bekommen SharePoint-Administratoren die Copilot-bezogenen Funktionen von SharePoint Advanced Management, sobald mindestens einer Person im Tenant eine Copilot-Lizenz zugewiesen ist.

Darf Copilot für Arztbriefe oder Befunde genutzt werden?

Das ist nicht Thema dieses Beitrags. Medizinische Einsatzfelder berühren Medizinprodukterecht und Haftung und brauchen eine eigene Bewertung. Für Verwaltung, QM und Leitung schließen Sie sie in den Einsatzregeln aus.

Wer sollte Copilot zuerst bekommen?

Personen mit hohem Nutzen und überschaubarem Risiko, typischerweise Qualitätsmanagement und Controlling. Personalabteilung und ärztliche Leitung folgen, wenn ihre Bestände bereinigt sind. Die Station steht in der Regel nicht am Anfang.

Muss die Vertretung zustimmen?

In aller Regel ja, weil Copilot zur Überwachung von Verhalten oder Leistung geeignet ist. Welche Vorschrift gilt, hängt von der Trägerschaft und beim Personalvertretungsrecht vom Bundesland ab. Binden Sie die Vertretung vor dem Piloten ein.

Fazit: Erst aufräumen, dann einschalten

Copilot im Krankenhaus ist kein Lizenzthema, sondern ein Berechtigungsthema mit Lizenzanhang. Die Werkzeuge, um es sauber zu machen, liefert Microsoft inzwischen selbst: Berichte zur Datenzugriffs-Governance, das Content Management Assessment, Restricted Access Control, Restricted Content Discovery, Vertraulichkeitsbezeichnungen und DLP für Copilot. Was Microsoft nicht liefern kann, ist die Entscheidung, welche Bestände in Ihrem Haus wohin gehören, und die Klarheit, dass Patientendaten ins KIS gehören und nicht in den Teams-Kanal.

Wer die Reihenfolge einhält, also prüfen, ausschließen bzw. kennzeichnen, pilotieren, ausrollen, und die Vertretung von Anfang an beteiligt, bekommt ein Werkzeug, das in Verwaltung, Qualitätsmanagement und Leitung spürbar Arbeit abnimmt. Wer die Reihenfolge abkürzt, bekommt einen sehr schnellen Suchdienst für alles, was im Haus seit Jahren zu weit geteilt ist. Wenn Sie wissen wollen, wo Ihr Haus steht, unterstützt Sie die Microsoft-365-Beratung für Krankenhäuser mit der Copilot- und Oversharing-Überprüfung. Technische Vertiefungen finden Sie in den Kompetenzbereichen Microsoft 365 Copilot, Microsoft Purview und SharePoint.

Weiter: Passende Beiträge und Kompetenzbereiche

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

› Teams im Krankenhaus: Gremien, Projekte, Kommissionen und wo Teams nichts zu suchen hat

› Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft

› § 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen

› Lizenzen im Krankenhaus: Frontline für die Pflege, Vollausstattung für die Verwaltung

› Microsoft 365 Security