

Microsoft 365 im Krankenhaus: Warum die Klinik anders tickt als Verwaltung und Mittelstand

Microsoft 365 · Krankenhaus und Klinikverbund · Einordnung

Microsoft 365 im Krankenhaus: Warum die Klinik anders tickt als Verwaltung und Mittelstand

Ein Haus, das nie schläft, drei Welten unter einem Dach und ein Gesetzbuch als Hausordnung.

24/7 ohne Wartungsfenster KIS und Subsysteme Medizintechnik im Netz Schichtdienst § 391 SGB V

§ 393 SGB V B3S Trägervielfalt

boddenberg.de



WISSEN

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

› [Microsoft 365 im Krankenhaus](#)

BERATUNG

Grobkonzept, Workshops und Begleitung für Krankenhäuser und Klinikverbünde, von der Tenant-Strategie bis zum QM-Handbuch.

› [Beratung für Krankenhäuser](#)

SCHULUNG

Für Klinik-IT, QM und Verwaltung: Microsoft 365 so lernen, wie es im Krankenhaus tatsächlich gebraucht wird.

› [Schulung für Krankenhäuser](#)

Wer Microsoft 365 schon im Mittelstand oder in einer Kommunalverwaltung eingeführt hat, kommt mit einem gewissen Selbstbewusstsein ins Krankenhaus. Tenant, Lizenzen, Teams-Struktur, Berechtigungskonzept, ein paar Workshops, fertig. Dieses Selbstbewusstsein hält ungefähr bis zur ersten Frage der Pflegedirektion, wann denn die Umstellung stattfindet. Die ehrliche Antwort lautet: Es gibt keinen Zeitpunkt, an dem niemand arbeitet. Das Haus schläft nicht, und es wartet auch nicht, bis die IT fertig ist.

Dieser Beitrag ordnet ein, warum ein Krankenhaus aus IT-Sicht anders tickt als ein Unternehmen oder eine Behörde, und was daraus für Microsoft 365 folgt. Es geht um den Betrieb rund um die Uhr, um KIS, Subsysteme und Medizintechnik als eigentliches Rückgrat, um drei Welten mit völlig unterschiedlichen Anforderungen unter einem Dach, um die Trägervielfalt mit ihrem jeweils eigenen Datenschutz- und Mitbestimmungsrecht und um eine Regulierungsdichte, bei der selbst erfahrene Datenschutzbeauftragte gelegentlich nachschlagen müssen. Er richtet sich an IT-Leitungen und Administratoren, Geschäftsführungen und kaufmännische Direktoren, Informationssicherheits-, Datenschutz- und Qualitätsmanagementbeauftragte, die Medizintechnik sowie Betriebsräte, Personalräte und Mitarbeitervertretungen.

Die Grundhaltung vorweg, weil sie sich durch die ganze Serie zieht: Patientendaten gehören ins KIS und seine Subsysteme. Microsoft 365 ist das Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Wer diese Grenze von Anfang an sauber zieht, erspart sich später die unangenehmsten Gespräche.

Was ein Krankenhaus aus IT-Sicht besonders macht

Ein Krankenhaus ist gleichzeitig Hotel, Labor, Hochleistungsbetrieb, Behörde mit Dokumentationspflicht, Ausbildungsstätte und Großküche. Jeder dieser Teile hat eigene Systeme,

eigene Hersteller und eigene Vorstellungen davon, was Verfügbarkeit bedeutet. Die IT verbindet das alles, und sie wird erst dann bemerkt, wenn sie es nicht mehr tut.

Die folgende Tabelle stellt die drei Umgebungen gegenüber, aus denen Microsoft-365-Projekte üblicherweise kommen. Sie ist bewusst zugespitzt. Es gibt Mittelständler mit Schichtbetrieb und Rathäuser mit Rund-um-die-Uhr-Diensten. In der Summe der Merkmale steht das Krankenhaus aber ziemlich allein da.

Merkmal	Mittelstand	Kommunalverwaltung	Krankenhaus
Betriebszeiten	Werktags, Wartung am Wochenende	Dienstzeiten, Wartung abends	Rund um die Uhr, an 365 Tagen, ohne echtes Wartungsfenster
Führendes System	ERP	Fachverfahren je Amt	KIS mit Dutzenden Subsystemen (LIS, RIS, PACS und weitere)
Geräte im Netz	PCs, Drucker, Maschinen	PCs, Drucker, Bürgerterminals	Zusätzlich Medizintechnik mit Herstellerfreigaben und langer Lebensdauer
Arbeitsplätze	Überwiegend persönlich	Überwiegend persönlich	Viele gemeinsam genutzte Stationsrechner, Schichtwechsel, schneller Benutzerwechsel
Sensibelste Daten	Geschäftsgeheimnisse, Personaldaten	Bürgerdaten, Personalakten	Gesundheitsdaten nach Art. 9 DSGVO, Schweigepflicht nach § 203 StGB
Datenschutzrecht	DSGVO, BDSG	DSGVO, Landesdatenschutzgesetz	DSGVO plus Landeskrankenhausgesetz, je nach Träger Landes-, Bundes- oder Kirchenrecht
Mitbestimmung	Betriebsrat	Personalrat	Betriebsrat, Personalrat oder Mitarbeitervertretung, je nach Träger
IT-Sicherheitspflichten	Je nach Größe NIS-2 über das BSIG	Landesrecht, teils IT-Grundschutz	§ 391 SGB V oder BSIG, B3S als Branchenstandard
Cloud-Vorgaben	Vertrag und DSGVO	Vertrag, DSGVO, Landesvorgaben	Zusätzlich § 393 SGB V mit C5-Testat für Gesundheitsdaten
Qualitätsmanagement	Oft ISO 9001	Selten formal	Verpflichtend nach QM-Richtlinie des G-BA, oft KTQ oder ISO 9001
Telefonie	Teams-Telefonie als Ablösung denkbar	Teams-Telefonie als Ablösung denkbar	Klinik-TK mit DECT, Zentrale und Patiententelefonie bleibt führend
Organisation	Ein Chef, eine Linie	Verwaltungsvorstand, Ämter	Geschäftsführung, Ärztlicher Direktor, Pflegedirektion, oft mehrere Standorte

FAKTEN · Größenordnung der deutschen Krankenhauslandschaft

Nach den Grunddaten des Statistischen Bundesamtes, veröffentlicht am 6. November 2025, gab es im Jahr 2024 in Deutschland 1.841 Krankenhäuser mit im Jahresdurchschnitt rund 472.900 Betten, davon rund 26.000 Intensivbetten. Behandelt wurden rund 17,5 Millionen Patienten vollstationär, die durchschnittliche Verweildauer lag bei 7,1 Tagen, die Bettenauslastung bei 72,0 Prozent.

Nach Trägerschaft: 528 Häuser in öffentlicher, 575 in freigemeinnütziger und 738 in privater Trägerschaft. Gemessen an den Betten sieht das Bild anders aus: Öffentliche Häuser stellen 46,8 Prozent, freigemeinnützige 32,3 Prozent und private 20,9 Prozent der Betten. Die Privaten betreiben also viele, im Schnitt aber kleinere Häuser.

Ende 2024 arbeiteten rund 217.700 Personen im ärztlichen Dienst und rund 1,24 Millionen im nichtärztlichen Dienst, davon rund 553.400 im Pflegedienst. Zusammen sind das erstmals seit 1991 mehr als eine Million Vollzeitäquivalente. Vorsorge- und Rehabilitationseinrichtungen weist die Statistik gesondert aus.

Zur Abgrenzung: Arztpraxen, Pflegeheime, ambulante Pflegedienste und Krankenkassen sind nicht Gegenstand dieser Serie. Sie unterliegen teils anderen Vorschriften, für Praxen etwa § 390 SGB V statt § 391, und haben einen völlig anderen Betrieb. Gemeint sind hier Akutkrankenhäuser aller Trägerschaften, Klinikverbünde mit mehreren Standorten, Fach- und Rehakliniken sowie Universitätsklinika.

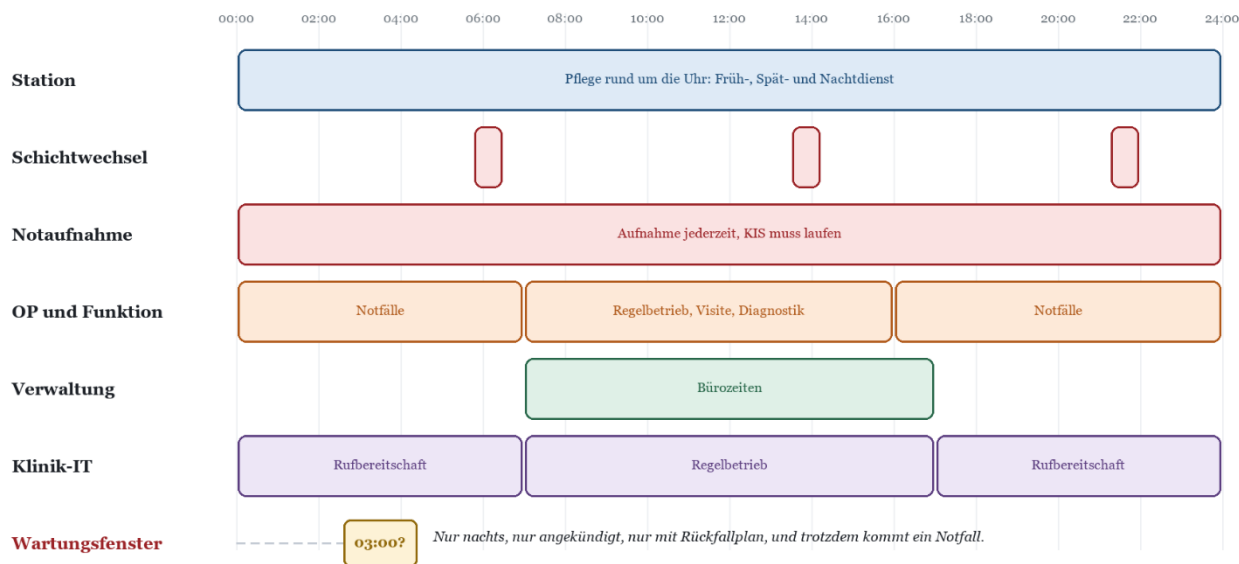
Betrieb ohne Feierabend: Rund um die Uhr, Schichtdienst, gemeinsame Rechner

Das Wartungsfenster, das es nicht gibt

Im Mittelstand ist Samstagnacht die Zeit für Updates. In der Kommunalverwaltung ist es der Abend nach Dienstschluss. Im Krankenhaus ist um drei Uhr nachts eine Notaufnahme geöffnet, auf jeder Station läuft der Nachtdienst, und irgendwo wird gerade ein Notfall-OP vorbereitet. Wer dort das KIS, den Terminalserver oder die Anmeldung am Stationsrechner anfasst, greift in einen laufenden Betrieb ein.

24 Stunden Krankenhaus: Wann ist hier eigentlich Wartungsfenster?

Typische Lage, je Haus verschieden. Die Suche nach der ruhigen Stunde bleibt erfolglos.



Skizze: Betrieb rund um die Uhr. Jede Wartung ist ein Eingriff am laufenden Haus.

Für Microsoft 365 klingt das zunächst entspannt: Den Dienst betreibt Microsoft, Updates kommen aus der Cloud, die Klinik-IT muss nachts nicht aufstehen. Ganz so einfach ist es nicht. Die Abhängigkeiten liegen lokal. Wenn die Synchronisation der Identitäten hängt, wenn ein Zertifikat abläuft oder wenn eine neue Richtlinie für bedingten Zugriff die Anmeldung am gemeinsam genutzten Rechner verhindert, steht nicht der Tenant still, sondern die Station. Änderungen an Identität und Anmeldung brauchen deshalb im Krankenhaus dieselbe Sorgfalt wie Änderungen am

KIS: angekündigt, abgestimmt, mit Rückfallplan und mit jemandem in Rufbereitschaft, der den Rückfallplan auch kennt.

TIPP · Change-Fenster mit der Pflegedirektion abstimmen

Legen Sie gemeinsam mit Pflegedirektion und Ärztlichem Direktor fest, welche Zeiten für Änderungen mit Auswirkungen auf Anmeldung und Arbeitsplätze akzeptabel sind. Meist sind das nicht die Nachtstunden, sondern ruhige Phasen am Vormittag nach der Visite, weil dann genug Personal da ist, um Probleme zu melden und Ausweichwege zu nutzen. Schichtwechsel sind dagegen tabu: Dort melden sich alle gleichzeitig an und wieder ab.

Schichtdienst und gemeinsam genutzte Rechner

Der Stationsrechner gehört niemandem. Er gehört der Station. Morgens um sechs übergibt der Nachtdienst an den Frühdienst, und innerhalb weniger Minuten arbeiten dort nacheinander Pflegekräfte, Stationsärzte, Auszubildende und vielleicht noch die Stationssekretärin. Wer das Konzept eines persönlichen Notebooks mit eigenem Profil, eigener OneDrive-Synchronisation und Outlook im Hintergrund auf diesen Arbeitsplatz überträgt, produziert Anmeldezeiten, die auf Station niemand akzeptiert, und zu Recht.

Daraus folgen Fragen, die sich in anderen Branchen so nicht stellen: Wie schnell muss ein Benutzerwechsel gehen? Reicht ein Terminalserver oder eine virtuelle Umgebung, die ohnehin für das KIS genutzt wird? Wer braucht überhaupt ein eigenes Postfach, wer eine Frontline-Lizenz mit schlankerem Funktionsumfang, wer gar nichts aus Microsoft 365? Und was passiert mit Dateien, die jemand auf dem gemeinsamen Rechner speichert, bevor er sich abmeldet, oder eben nicht abmeldet?

Rufbereitschaft auch für die IT

Die Klinik-IT ist meist klein im Verhältnis zur Zahl der Arbeitsplätze und Systeme. Außerhalb der Bürozeiten gibt es Rufbereitschaft, und die deckt in der Regel KIS, Netz und Server ab. Microsoft 365 kommt oft erst später dazu, und mit ihm die Frage, wer nachts ein gesperrtes Konto entsperrt oder einen kompromittierten Zugang stilllegt. Wer Microsoft 365 einführt, sollte diese Frage beantworten, bevor die erste Pflegekraft nachts vor einer Sperrmeldung steht.

KIS, Subsysteme, Medizintechnik: Wo Microsoft 365 hingehört

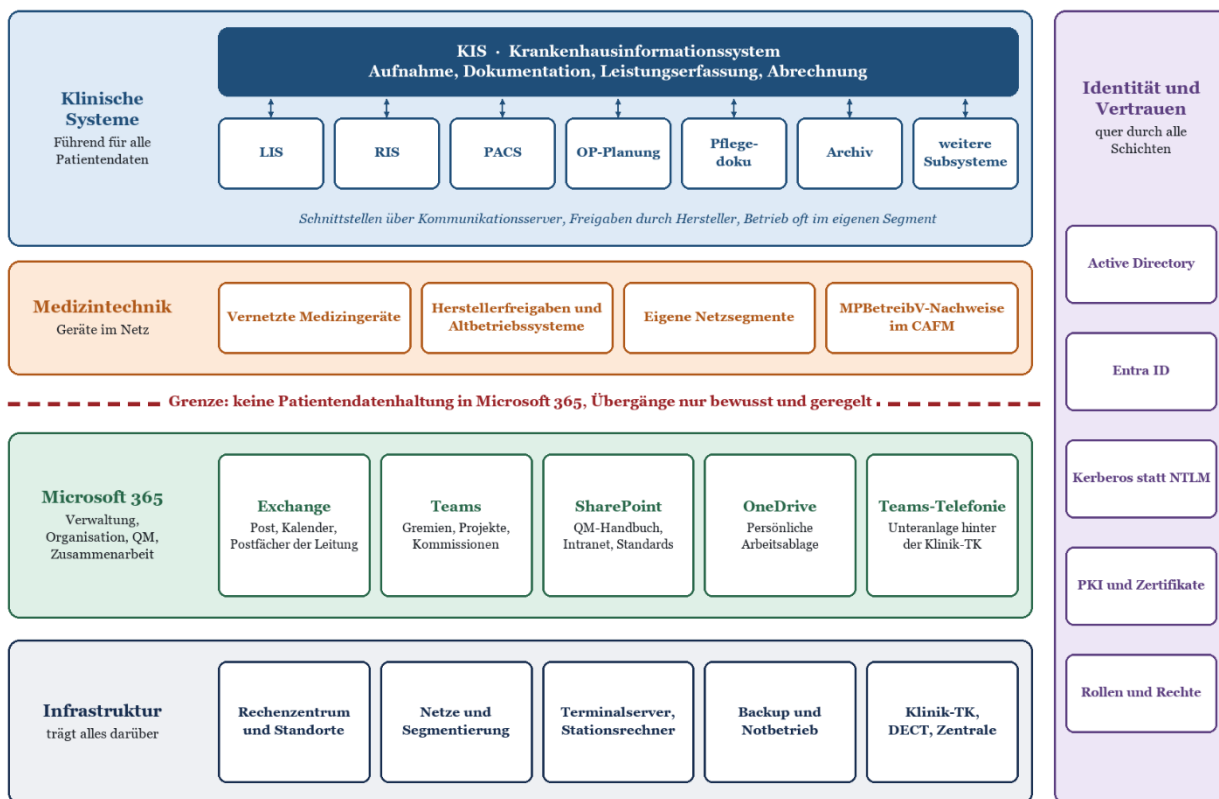
Das eigentliche Rückgrat

Im Mittelstand ist Microsoft 365 oft das wichtigste System nach dem ERP. Im Krankenhaus ist es das nicht, und es sollte auch nicht so tun. Das Rückgrat ist das KIS mit seinen Subsystemen: Laborinformationssystem, Radiologieinformationssystem, PACS, OP-Planung, Pflegedokumentation, Archiv und je nach Haus Dutzende weitere Anwendungen, die über einen Kommunikationsserver miteinander sprechen. Viele davon laufen auf Datenbanken, die niemand im Haus selbst entworfen hat, und alle haben Hersteller, die bei Updates von Betriebssystem oder Datenbank mitreden.

Das prägt die IT-Abteilung. Sie verbringt einen erheblichen Teil ihrer Zeit damit, Herstellerfreigaben abzuwarten, Schnittstellen zu überwachen und Anwendungen zu betreiben, die sie nicht ändern darf. Microsoft 365 ist in diesem Gefüge ein weiteres System, das sich einordnen muss: neben dem KIS, nicht an seiner Stelle.

Das Krankenhaus als Schichtenmodell

Patientendaten leben im KIS und seinen Subsystemen. Microsoft 365 arbeitet daneben, nicht darin.



Skizze: Vier Schichten, eine Querspange. Die rote Linie ist die wichtigste im ganzen Bild.

Die Skizze zeigt das Schichtenmodell, mit dem sich die meisten Diskussionen ordnen lassen. Oben die klinischen Systeme, die für alle Patientendaten führend sind. Darunter die Medizintechnik mit ihren eigenen Netzsegmenten und Regeln. Dann die rote Linie. Unter ihr Microsoft 365 als Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit, ganz unten die Infrastruktur, die alles trägt. Quer durch alle Schichten laufen Identität und Vertrauen: Active Directory, Entra ID, Kerberos und eine PKI, ohne die weder das KIS noch Microsoft 365 sicher funktionieren.

Information	Gehört in	Microsoft 365 darf	Anmerkung
Befunde, Bilder, Pflegedokumentation	KIS und Subsysteme	Nichts	Die Patientenakte ist und bleibt im KIS
Belegungs- und Übergabelisten mit Namen	KIS (Stationsansichten, Berichte)	Im Grundsatz nichts	Klassischer Kandidat für die Excel-Liste in Teams, siehe Warnung
QM-Handbuch, Verfahrensweisungen, Standards	SharePoint mit Dokumentenlenkung	Führend sein	Freigabe, Versionierung, Nachweis für das Audit
Hygieneplan, Notfallpläne	SharePoint, zusätzlich Papier für den Notbetrieb	Führend sein	Auffindbarkeit auf Station ist das Kriterium
Gremien, Kommissionen, Projekte	Teams und SharePoint	Führend sein	Ohne Patientenbezug oder pseudonymisiert
Verwaltungskorrespondenz	Exchange und SharePoint	Führend sein	Aufbewahrungsfristen mit Purview abbilden

Geräteakten, Einweisungen	CAFM bzw. Medizintechnik-Software	Ergänzen	MPBetreibV-Nachweise nicht doppelt führen
----------------------------------	-----------------------------------	----------	---

WARNUNG · Die Excel-Liste mit Patientennamen im Teams-Kanal

Sie existiert. In vielen Häusern. Eine Übergabeliste, eine Belegungsübersicht für die Bettenkoordination, eine Liste für die Entlassplanung, angelegt, weil das KIS die gewünschte Ansicht nicht hergab oder weil es schnell gehen musste. Dann wurde sie in Teams geteilt, weil das bequemer ist als ein Netzlaufwerk. Und plötzlich liegen Gesundheitsdaten in einem Cloud-Dienst, für den es weder eine Rechtsgrundlage noch eine Prüfung nach § 393 SGB V noch eine Löschregel gibt.

Das ist nicht der Normalfall und darf keiner werden. Es ist aber die Realität, mit der jede Einführung rechnen muss. Die Antwort ist nicht der erhobene Zeigefinger, sondern eine bessere Lösung im KIS, eine klare Regel im Nutzungskonzept und technische Leitplanken mit Microsoft Purview, die solche Inhalte erkennen und sichtbar machen.

Medizintechnik im Netz

Medizingeräte sind langlebig, teuer und zertifiziert. Ein Gerät, das zehn Jahre und länger im Einsatz ist, bringt sein Betriebssystem und seine Protokolle mit, und der Hersteller entscheidet, ob und wann ein Update zulässig ist. Für die Klinik-IT heißt das: Segmentierung statt Patchen, Ausnahmen statt einheitlicher Härtung, und viel Abstimmung mit der Medizintechnik, die organisatorisch oft gar nicht zur IT gehört.

Für Microsoft 365 ist das relevant, weil Härtungsmaßnahmen im Verzeichnisdienst und in der Anmeldung die Medizintechnik unmittelbar treffen. Wer im Zuge der Sicherheitsarbeit NTLM abschalten oder die Anforderungen an Kerberos verschärfen will, stößt früher oder später auf ein Gerät oder eine Altanwendung, die genau das nicht kann.

TYPISCHE SITUATION · Aus der Projektpraxis

In der langjährigen Begleitung eines Krankenhausverbunds mit mehreren Standorten ging es um Vertrauensstellungen zwischen Domänen, die Abschaltung von NTLM und die Umstellung auf Kerberos, den Aufbau und die Härtung einer PKI, Exchange Hybrid, eine SQL-Performance-Analyse für eine Medizintechnik- und CAFM-Anwendung sowie forensische Arbeit. Die Erkenntnis, die sich durch alle diese Themen zieht: Im Krankenhaus ist keine Infrastrukturänderung nur eine Infrastrukturänderung. Am anderen Ende hängt immer ein Funktionsbereich, eine Station oder ein Gerät.

Mehr zu den technischen Grundlagen in den Kompetenzbereichen [Kerberos](#), [PKI mit Active Directory Certificate Services](#) und [SQL Server](#).

Telefonie: Unteranlage, nicht Ablösung

Ein Wort zur Telefonie, weil die Frage in jedem Projekt kommt. Im Mittelstand kann Teams-Telefonie die alte Anlage vollständig ablösen. Im Krankenhaus bleibt die große Klinik-TK-Anlage mit DECT, Zentrale, Alarmierung und Patiententelefonie führend. Teams-Telefonie ist dort in aller Regel eine Unteranlage für die Verwaltung und für ärztliche Leitungspositionen, die ohnehin viel in Teams arbeiten. Das ist kein Kompromiss, sondern die passende Architektur. Mehr dazu unter [Teams-Telefonie im Krankenhaus und in der Pflege](#).

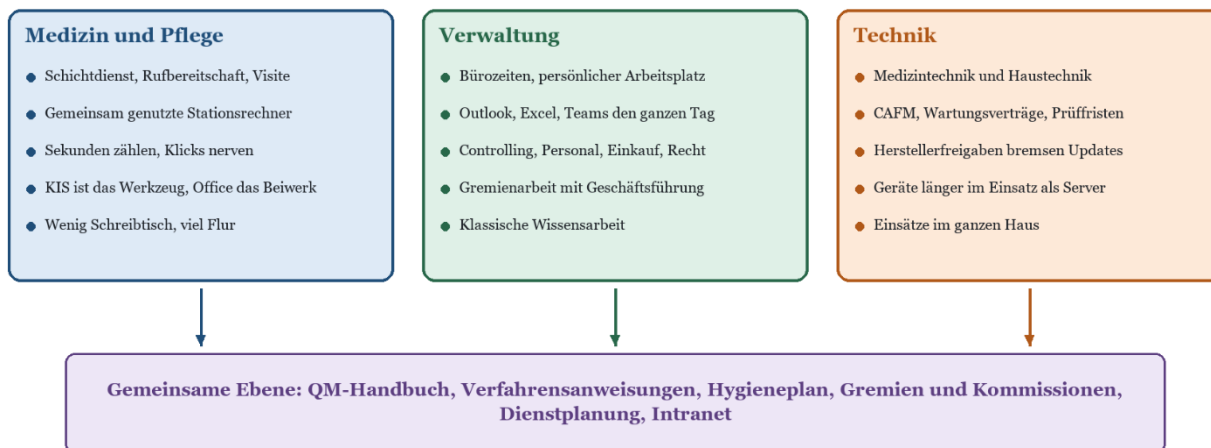
Drei Welten und viele Träger

Medizin und Pflege, Verwaltung, Technik

Im Krankenhaus arbeiten drei Welten unter einem Dach, die sich in fast allem unterscheiden, was für die IT zählt: Arbeitszeit, Arbeitsplatz, Werkzeuge, Geduld mit Technik. Die Verwaltung arbeitet wie jede andere Verwaltung, nur mit Krankenhausvokabular. Medizin und Pflege arbeiten im Schichtdienst, am Patienten, auf dem Flur und am gemeinsamen Rechner. Die Technik pendelt zwischen Werkstatt, Station und Hersteller-Hotline.

Drei Welten unter einem Dach

Gleiches Haus, gleicher Tenant, völlig unterschiedliche Arbeitstage.



Ein Konzept, das nur eine der drei Welten kennt, scheitert an den beiden anderen.

Skizze: Die drei Welten im Krankenhaus und ihre gemeinsame Schnittmenge.

Anforderung	Medizin und Pflege	Verwaltung	Technik
Arbeitsplatz	Gemeinsam genutzt, mobil, Visitenwagen	Persönlich, Büro	Wechselnd, Werkstatt und Station
Anmeldung	Schnell, oft mit Karte oder Token	Klassisch mit MFA	Klassisch, teils auf Fremdgeräten
Typische Microsoft-365-Nutzung	Intranet, Standards, Dienstpläne, Kommunikation	Vollumfänglich	Dokumentation, Abstimmung mit Herstellern
Lizenzbedarf	Häufig Frontline	Vollausstattung	Je nach Rolle
Schulungsform	Kurz, stationsnah, schichtkompatibel	Klassische Schulung	Praxisnah, an konkreten Abläufen
Größte Sorge	Zeitverlust am Patienten	Datenschutz, Ablage, Fristen	Gerätefreigaben, Verfügbarkeit

Dazwischen liegt die gemeinsame Ebene, auf der Microsoft 365 seinen größten Nutzen stiftet: das QM-Handbuch mit Verfahrensanweisungen und Standards, der Hygieneplan, die Arbeit in Gremien und Kommissionen, das Intranet. Hier ist SharePoint tatsächlich das richtige Werkzeug, und hier liegt auch eigene Projekterfahrung: QM-Handbücher mit SharePoint für ein Krankenhaus, mit Dokumentenlenkung, die im Zertifizierungsaudit nach KTQ oder ISO 9001 trägt. Wie das grundsätzlich funktioniert, beschreibt die Seite zur [Dokumentenlenkung nach ISO 9001](#).

Trägervielfalt: Wer mitbestimmt und welches Recht gilt

Die zweite Besonderheit ist die Vielfalt der Träger. Ein kommunales Haus, ein kirchliches Haus und ein Haus eines privaten Konzerns können im selben Landkreis stehen, dieselben Patienten versorgen und dasselbe KIS nutzen und trotzdem unter völlig verschiedenen Regeln für Datenschutz und Mitbestimmung arbeiten.

Trägerschaft	Datenschutzrecht neben der DSGVO	Mitbestimmung	Besonderheit
Öffentlich, in öffentlich-rechtlicher Form	Landesdatenschutzgesetz, Landeskrankenhausgesetz	Personalrat nach Landespersonalvertretungsrecht	Kommunale Aufsicht, Vergaberecht
Öffentlich, als GmbH	BDSG, Landeskrankenhausgesetz	Betriebsrat nach BetrVG	Kommune als Gesellschafter, oft Vergaberecht
Freigemeinnützig, kirchlich	KDG (katholisch) oder DSG-EKD (evangelisch), kirchliche Aufsicht	Mitarbeitervertretung nach MAVO oder MVG	Eigene Datenschutzaufsicht der Kirche
Freigemeinnützig, nicht kirchlich	BDSG, Landeskrankenhausgesetz	Betriebsrat, teils Tendenzschutz	Wohlfahrtsverband als Dach
Privat	BDSG, Landeskrankenhausgesetz	Betriebsrat, oft Konzernbetriebsrat	Konzernvorgaben, häufig zentraler Tenant
Universitätsklinikum	Je nach Rechtsform Landes- oder Bundesrecht	Personalrat oder Betriebsrat	Verflechtung mit Hochschule und Forschung

Hinzu kommt das Landesrecht. Die Landeskrankenhausgesetze regeln den Umgang mit Patientendaten unterschiedlich detailliert, manche mit eigenen Vorgaben zur Datenverarbeitung im Auftrag, andere zurückhaltender. Auch das Personalvertretungsrecht unterscheidet sich von Land zu Land, etwa darin, wie weit die Mitbestimmung bei technischen Einrichtungen reicht. Ein Konzept, das in einem Bundesland passt, lässt sich nicht ungeprüft ins Nachbarland übertragen, und für einen Klinikverbund mit Standorten in mehreren Ländern ist das keine akademische Frage.

Wer aus der Kommunalverwaltung oder aus dem kirchlichen Bereich kommt, findet manches wieder, was dort schon gilt. Die Kompetenzbereiche [Microsoft 365 in der öffentlichen Verwaltung](#) und [Microsoft 365 in Kirche, Diakonie und Caritas](#) beschreiben diese Grundlagen, Universitätsklinika finden Anknüpfungspunkte unter [Microsoft 365 in Hochschule und Forschung](#).

HINWEIS · Keine Rechtsberatung

Welches Datenschutzrecht, welches Landeskrankenhausgesetz und welches Mitbestimmungsrecht für Ihr Haus gilt, hängt von Trägerschaft, Rechtsform und Bundesland ab. Dieser Beitrag ordnet ein und ersetzt keine rechtliche Prüfung. Ziehen Sie Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten, das Justizariat und bei Bedarf externe Rechtsberatung frühzeitig hinzu, und zwar vor der ersten Pilotgruppe, nicht danach.

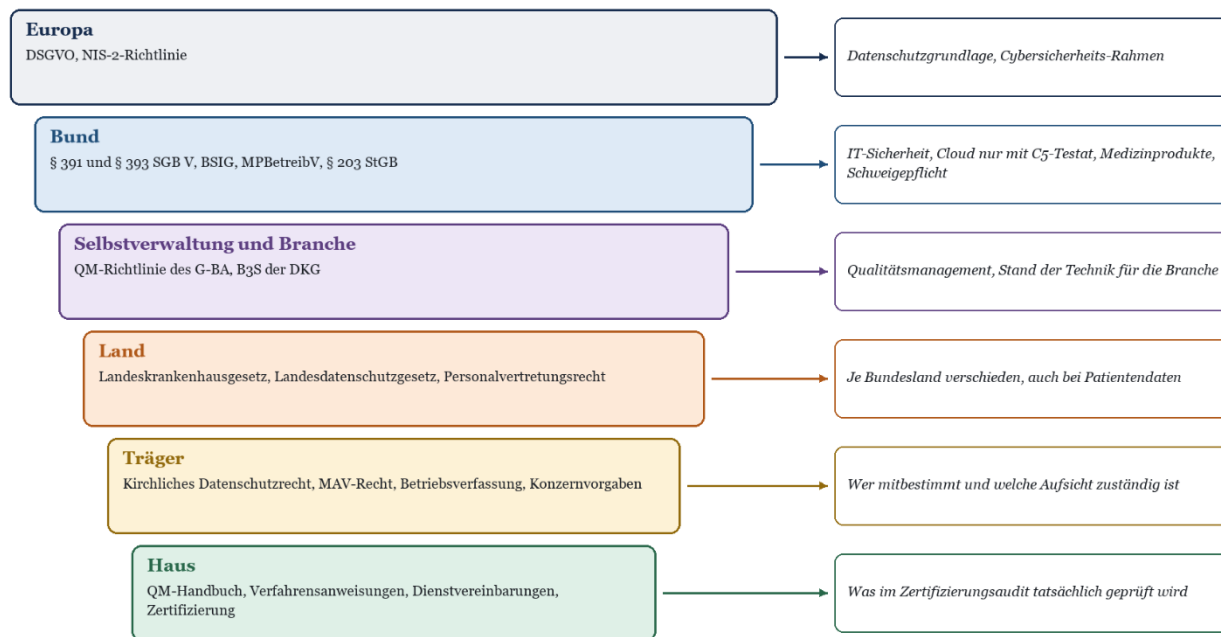
Regulierungsdichte: Von § 391 SGB V bis zur QM-Richtlinie

Kaum eine Branche hat so viele Regelwerke, die gleichzeitig auf dieselbe IT wirken. Ein Mittelständler kennt meist die DSGVO und, je nach Größe, inzwischen das BSIG. Ein Krankenhaus hat dazu das Sozialgesetzbuch, die Medizinprodukte-Betreiberverordnung, die Richtlinien des

Gemeinsamen Bundesausschusses, den Branchenstandard der Deutschen Krankenhausgesellschaft und das Recht seines Landes und seines Trägers.

Wer dem Krankenhaus alles etwas zu sagen hat

Vereinfachte Übersicht. Welche Ebene für Ihr Haus gilt, hängt von Größe, Land und Träger ab.



Skizze: Sechs Ebenen Regelwerk. Der Mittelstand kennt davon meist zwei.

IT-Sicherheit: § 391 SGB V, BSIG und NIS-2

§ 391 SGB V, früher § 75c, verpflichtet alle Krankenhäuser, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zu treffen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme zu vermeiden. Maßstab sind die Funktionsfähigkeit des Krankenhauses und die Sicherheit der Patienteninformationen. Dazu gehören ausdrücklich verpflichtende Maßnahmen zur Sensibilisierung der Belegschaft. Die Pflicht kann insbesondere erfüllt werden, indem ein branchenspezifischer Sicherheitsstandard angewendet wird, dessen Eignung das BSI festgestellt hat.

Seit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes am 6. Dezember 2025 gilt die Vorschrift in neuer Fassung. Für Krankenhäuser, die als Betreiber kritischer Anlagen eingestuft sind, gelten nicht § 391, sondern die Pflichten des BSI-Gesetzes. Nach den Informationen des BSI liegt der Schwellenwert für ein Krankenhaus als kritische Anlage weiterhin bei 30.000 vollstationären Fällen im Jahr. Darunter kann ein Haus je nach Größe als wichtige oder besonders wichtige Einrichtung unter das BSIG fallen, mit Registrierungs- und Meldepflichten. Welche Kategorie für Ihr Haus gilt, prüfen Sie am besten mit der Betroffenheitsprüfung des BSI und mit Ihrem Justizariat. Wie sich die Pflichten technisch in Microsoft 365 abbilden lassen, beschreibt [NIS2 technisch umsetzen mit Microsoft 365](#).

Der Branchenstandard B3S „Medizinische Versorgung“ der DKG liegt in Version 1.3 vom 10. Oktober 2025 vor, deren Eignung das BSI im November 2025 festgestellt hat; die DKG stellt inzwischen eine redaktionell überarbeitete Fassung 1.3.1 bereit. Für die Microsoft-365-Einführung ist der B3S der Maßstab, an dem sich Informationssicherheitsbeauftragte und Auditoren orientieren. Wer Microsoft 365 einführt, sollte die relevanten Anforderungen von Anfang an auf Tenant-Konfiguration, Identitätsschutz und Protokollierung abbilden. Der Kompetenzbereich [Microsoft 365 Security](#) gibt dafür den technischen Überblick.

Cloud: § 393 SGB V und das C5-Testat

§ 393 SGB V erlaubt Leistungserbringern, also auch Krankenhäusern, die Verarbeitung von Sozial- und Gesundheitsdaten in Cloud-Diensten, aber nur unter Bedingungen. Die Verarbeitung muss im Inland, in der EU, einem gleichgestellten Staat oder einem Drittstaat mit Angemessenheitsbeschluss stattfinden, die verarbeitende Stelle braucht eine Niederlassung in Deutschland, und seit dem 1. Juli 2025 ist ein aktuelles C5-Typ-2-Testat für die eingesetzten Cloud-Systeme erforderlich, sofern nicht ein gleichwertiges Testat oder Zertifikat nach der Verordnung des Bundesgesundheitsministeriums vorliegt. Zusätzlich müssen die im Testat genannten kundenseitigen Kriterien umgesetzt sein, und das ist der Teil, den viele übersehen.

WICHTIG · Prüfauftrag statt Annahme

Welche Microsoft-Dienste von welchem C5-Testat welchen Typs abgedeckt sind, lässt sich nicht pauschal beantworten und ändert sich mit jedem Prüfzyklus. Prüfen Sie den aktuellen Stand selbst im Service Trust Portal von Microsoft, gleichen Sie den Prüfumfang mit den Diensten ab, die Sie tatsächlich nutzen wollen, und dokumentieren Sie, wie Sie die kundenseitigen Kriterien umsetzen.

Einstieg: [Microsoft Service Trust Portal](#).

Und selbst wenn das Testat passt: § 393 regelt die Voraussetzungen für den Cloud-Einsatz, nicht die Frage, ob Patientendaten in Teams gehören. Die Grundhaltung dieser Serie bleibt.

Medizinprodukte und Qualitätsmanagement

Die Medizinprodukte-Betreiberverordnung verlangt Nachweise zu Einweisungen, Prüfungen und Bestand der Medizinprodukte. Diese Dokumentation lebt in der Regel in einer CAFM- oder Medizintechnik-Software, und dort sollte sie auch führend bleiben. SharePoint kann ergänzen, etwa für Verfahrensanweisungen und Schulungsunterlagen, darf die Nachweisführung aber nicht verdoppeln.

Die Qualitätsmanagement-Richtlinie des G-BA verpflichtet Krankenhäuser zu einem einrichtungsinternen Qualitätsmanagement. Viele Häuser lassen sich zusätzlich nach KTQ oder ISO 9001 zertifizieren. Für Microsoft 365 ist das die vielleicht dankbarste Regulierung: Dokumentenlenkung, Freigabe, Versionierung und Nachweis gehören zu den Dingen, die SharePoint richtig gut kann, wenn man es richtig aufsetzt. Dazu kommen Aufbewahrungsfristen für Verwaltungsunterlagen, die sich mit [Microsoft Purview](#) abbilden lassen, ausdrücklich nicht für die Patientenakte.

Regelwerk	Worum es geht	Bedeutung für Microsoft 365
§ 391 SGB V	IT-Sicherheit nach Stand der Technik für alle Krankenhäuser, soweit nicht KRITIS	Härtung, Identitätsschutz, Sensibilisierung, Notfallplanung einbeziehen
BSIG (NIS-2)	Pflichten für kritische Anlagen sowie wichtige und besonders wichtige Einrichtungen	Registrierung, Meldewege, Risikomanagement auch für Cloud-Dienste
B3S der DKG	Branchenstandard, vom BSI als geeignet festgestellt	Maßstab für Konfiguration und Nachweis im Audit
§ 393 SGB V	Cloud-Verarbeitung von Gesundheitsdaten nur mit aktuellem C5-Testat	Prüfauftrag je Dienst, kundenseitige Kriterien umsetzen
§ 203 StGB	Schweigepflicht, auch bei Einbindung von Dienstleistern	Verträge und Verpflichtungen prüfen
MPBetreibV	Betrieb, Prüfung und Dokumentation von Medizinprodukten	CAFM bleibt führend, SharePoint ergänzt

QM-Richtlinie des G-BA	Einrichtungsinternes Qualitätsmanagement	SharePoint als QM-Handbuch mit Dokumentenlenkung
Landesrecht	Landeskrankenhausgesetz, Datenschutz, Personalvertretung	Je Bundesland gesondert prüfen

Gilt § 391 SGB V auch für die Rehaklinik? Das hängt davon ab, ob die Einrichtung im Sinne des Gesetzes ein Krankenhaus ist oder eine Vorsorge- oder Rehabilitationseinrichtung. Die Frage klingt formal, entscheidet aber darüber, welcher Pflichtenkatalog greift, und sollte vor jedem Sicherheitskonzept geklärt sein.

Häufige Fragen zu Microsoft 365 im Krankenhaus

Dürfen Patientendaten in Microsoft 365 gespeichert werden?

Rechtlich ist der Cloud-Einsatz für Gesundheitsdaten unter den Voraussetzungen des § 393 SGB V und des jeweiligen Landesrechts nicht von vornherein ausgeschlossen. Die Empfehlung dieser Serie ist trotzdem eindeutig: Patientendaten gehören ins KIS und seine Subsysteme. Microsoft 365 ist für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit da. Die Einzelfallprüfung gehört zu Datenschutz und Justizariat.

Ersetzt Microsoft 365 das KIS oder Teile davon?

Nein. Das KIS ist für die Patientenversorgung führend und bleibt es. Microsoft 365 ergänzt dort, wo das KIS nicht zuständig ist: Gremienarbeit, Projekte, Intranet, QM-Handbuch, Verwaltungskorrespondenz.

Brauchen Pflegekräfte überhaupt Microsoft 365?

Viele brauchen Zugang zu Intranet, Standards, Dienstplänen und interner Kommunikation, aber kein volles Büropaket. Dafür gibt es Frontline-Lizenzen mit schlankerem Funktionsumfang. Welche Pläne für welche Rolle passen, sollte anhand der aktuellen Lizenzbeschreibungen von Microsoft und der tatsächlichen Arbeitsabläufe entschieden werden.

Wann kann man im Krankenhaus Änderungen einspielen?

Es gibt kein Wartungsfenster wie im Büro. Änderungen an Anmeldung und Arbeitsplätzen werden mit Pflegedirektion und Ärztlichem Direktor abgestimmt, angekündigt und mit Rückfallplan umgesetzt, möglichst nicht zum Schichtwechsel.

Löst Teams-Telefonie die Klinik-TK ab?

In aller Regel nicht. Station, DECT, Zentrale und Patiententelefonie bleiben an der Klinik-TK. Teams-Telefonie bietet sich als Unteranlage für Verwaltung und ärztliche Leitungspositionen an.

Ist Microsoft 365 für Krankenhäuser durch ein C5-Testat freigegeben?

Eine solche pauschale Freigabe gibt es nicht. § 393 SGB V verlangt ein aktuelles C5-Typ-2-Testat für die eingesetzten Systeme und die Umsetzung der kundenseitigen Kriterien. Welche Dienste abgedeckt sind, prüfen Sie im Service Trust Portal für Ihren konkreten Einsatz.

Wer muss bei der Einführung mitreden?

Geschäftsführung, IT-Leitung, Informationssicherheit, Datenschutz, Qualitätsmanagement, Pflegedirektion, Ärztlicher Direktor, Medizintechnik und die Arbeitnehmervertretung, also je nach Träger Betriebsrat, Personalrat oder Mitarbeitervertretung. Wer jemanden davon vergisst, lernt ihn spätestens in der dritten Projektsitzung kennen.

Gilt das alles auch für Arztpraxen oder Pflegeheime?

Nur sehr eingeschränkt. Praxen, Pflegeheime, ambulante Dienste und Krankenkassen haben andere Vorschriften und einen anderen Betrieb. Diese Serie richtet sich an Krankenhäuser und Klinikverbünde.

Fazit: Ein Haus, das nie schläft, verdient ein eigenes Konzept

Ein Krankenhaus ist kein großer Mittelständler mit Betten und keine Behörde mit OP-Sälen. Es läuft rund um die Uhr, sein Rückgrat ist das KIS mit seinen Subsystemen, seine Geräte haben Hersteller, die mitreden, seine Belegschaft arbeitet in drei Welten, sein Träger bestimmt, welches Recht gilt, und über allem liegt eine Regulierungsdichte, die selbst Juristen Respekt abnötigt. Wer Microsoft 365 dort mit der Vorlage aus dem letzten Industrieprojekt einführt, wird es merken, meist zuerst auf Station.

Das ist kein Grund, die Finger davon zu lassen. Für Verwaltung, Gremien, Qualitätsmanagement und Zusammenarbeit ist Microsoft 365 im Krankenhaus ein starkes Werkzeug, gerade weil die Anforderungen an Nachweis und Dokumentenlenkung so hoch sind. Entscheidend ist, die Grenze zum KIS sauber zu ziehen, die drei Welten getrennt zu denken und die Regelwerke von Anfang an mitzunehmen. Wie die einzelnen Themen im Detail aussehen, von Lizenzen über QM-Handbuch und Teams bis zur Sicherheit, zeigt die Übersichtsseite [Microsoft 365 im Krankenhaus](#). Wenn Sie für Ihr Haus oder Ihren Klinikverbund einen Startpunkt suchen, sprechen Sie uns über die [Microsoft-365-Beratung für Krankenhäuser](#) an.

WEITERLESEN • Weiterlesen

Passende Kompetenzbereiche zu diesem Beitrag:

- › [Microsoft Entra ID](#)
- › [Kerberos](#)
- › [PKI mit Active Directory Certificate Services](#)
- › [SharePoint](#)
- › [Dokumentenlenkung nach ISO 9001](#)
- › [Microsoft Purview](#)
- › [Microsoft 365 Security](#)
- › [NIS2 technisch umsetzen mit Microsoft 365](#)
- › [Teams-Telefonie im Krankenhaus und in der Pflege](#)
- › [Microsoft-365-Schulung für Krankenhäuser](#)