BOI BETTER ORGANIZED INFORMATION

WHITEPAPER



DATA GOVERNANCE IM KRANKENHAUS

Anforderungen an Prozesse
zur Bearbeitung kritischer Daten

www.boi.at

INHALT

Management Summary 3

Handlungsbedarf 4

Was sind kritische Daten? 5

Die drei Schutzziele 6

Regulatorischer Rahmen 7

Deutschland: BSIG / NIS2 8

Deutschland: B3S Krankenhaus 9

Österreich: NISG 2026 10

Vier Schutzstufen 11

Datenhaltung und Least-to-know-Prinzip 12

Kontrollierte Prozesse 13

Schnittstellen 13

Anforderungen an Software 14

Fazit und Ausblick 15

© All rights reserved - Stand: Oktober 2026

Management Summary

Mit zunehmender Digitalisierung wird der Krankenhausbetrieb immer stärker von der **Verfügbarkeit, Integrität und Vertraulichkeit digitaler Daten** abhängig. Dies betrifft neben Patienten- und Behandlungsdaten auch Daten für klinische und administrative Prozesse wie Kataloge und Terminologien, klinische Regeln, Scores und Assessments, Referenzwerte, Behandlungspfade, Dokumentationskonfigurationen, Interoperabilitäts-Mappings oder organisatorische und technische Konfigurationsdaten.

Im Mittelpunkt dieses Whitepapers stehen **diese prozesskritischen Daten** und die Anforderungen an ihre sichere Bearbeitung – nicht die Verarbeitung personenbezogener Patienten- und Behandlungsdaten.

Fehlerhafte, manipulierte oder nicht verfügbare Daten dieser Art können Prozesse erheblich beeinträchtigen und mittelbar Auswirkungen auf die Patientensicherheit haben. Sie sind daher als **kritische Daten** in das Informationssicherheits- und Risikomanagement eines Krankenhauses einzubeziehen.

Die regulatorischen Rahmenbedingungen in Deutschland und Österreich stellen entsprechend hohe Anforderungen an den Schutz kritischer Daten. Maßgeblich sind insbesondere die Anforderungen aus NIS2 und B3S Krankenhaus in Deutschland und dem nationalen NIS2-Rahmen in Österreich, die neben technischen Maßnahmen zwingend organisatorische Maßnahmen erfordern.

Im Kern verlangen diese Regelwerke ein **risikobasiertes Sicherheitsmanagement**. Krankenhäuser müssen kritische Daten und die davon abhängigen Prozesse identifizieren, Risiken und mögliche Auswirkungen bewerten, angemessene Schutzmaßnahmen implementieren und deren Wirksamkeit nachvollziehbar nachweisen.

Für die praktische Datenbewirtschaftung bedeutet dies: **Kritische Daten müssen über ihren gesamten Lebens- und Änderungszyklus kontrolliert werden.** Änderungen müssen autorisiert, validiert und nachvollziehbar sein. Gleichzeitig müssen Verfügbarkeit, Widerstandsfähigkeit und Wiederherstellbarkeit gewährleistet werden.



© All rights reserved - Stand: Oktober 2026

Handlungsbedarf

Eine besondere Herausforderung entsteht dort, wo Standard- und Businesssoftware die individuellen Anforderungen eines Krankenhauses nicht vollständig abbildet. Dies betrifft beispielsweise individuelle Kataloge und Prozesse, lokale Erweiterungen offizieller Kataloge und Terminologien sowie die Pflege von Referenz- und Konfigurationsdaten für Krankenhausinformationssysteme.

Wenn die Businesssoftware nicht an individuelle Anforderungen anpassbar oder die Umsetzung zu kostspielig ist, entstehen oft unkontrollierte Prozesse unter Verwendung von Microsoft Excel, E-Mail, Telefon und anderen Hilfsmitteln. Diese können die Einhaltung der Schutzziele für kritische Daten gefährden.

Eine weitere Herausforderung ist, dass diese unkontrollierten Prozesse nicht mit vor- oder nachgelagerten, automatisierten Prozessschritten synchronisierbar sind. Hierdurch entstehen häufig **Medienbrüche zwischen manueller Datenbearbeitung und automatisierten Prozessen.** Diese Übergänge müssen organisatorisch und technisch so gestaltet werden, dass Schutzziele durchgängig eingehalten und nachgewiesen werden können und effiziente Gesamtprozesse entstehen.



- **Unkontrollierte Prozesse**
  Individuelle Datenbearbeitung über Microsoft Excel, E-Mail und manuelle Abläufe
- **Verteilte Daten**
  Mehrere Datenquellen erschweren eine einheitliche Datenbearbeitung.
- **Medienbrüche**
  Manuelle Schritte unterbrechen automatisierte Prozessabläufe.
- **Fehlende Nachvollziehbarkeit**
  Änderungen und Freigaben sind nicht durchgängig dokumentiert.

Die zentrale Managementaufgabe besteht daher darin, für kritische Daten effiziente Prozesse mit automatischen und manuellen Schritten und durchgängiger Data Governance zu etablieren - vom fachlichen Änderungsbedarf bis zur produktiven Verwendung - einschließlich klarer Verantwortlichkeiten, kontrollierter Freigaben, vollständiger Nachvollziehbarkeit und sicherer technischer Integration.

© All rights reserved - Stand: Oktober 2026

Was sind kritische Daten?

Fragestellung und Abgrenzung

Dieses Whitepaper widmet sich der Frage, welche Anforderungen sich aus den Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit sowie den aktuellen regulatorischen Rahmenbedingungen in Deutschland und Österreich an sichere Bearbeitungsprozesse für kritische Daten und an entsprechende Softwarelösungen aus NIS2 ergeben.

Nicht Gegenstand der Betrachtung sind Patienten- oder sonstige personenbezogene Daten. Datenschutzrechtliche Anforderungen, insbesondere aus DSGVO, nationalem Datenschutzrecht oder Vorschriften über elektronische Patientenakten werden daher nicht betrachtet.

Der Begriff **kritische Daten** wird in diesem Whitepaper funktional verwendet und bezeichnet keine eigenständige gesetzliche Datenkategorie. Gemeint sind Informationen, deren **Fehlerhaftigkeit, unautorisierte Veränderung, Verlust, Nichtverfügbarkeit oder verspätete Aktualisierung** relevante Krankenhausprozesse erheblich beeinträchtigen können. Dadurch können technische, administrative und logistische Abläufe gestört und mittelbar auch die Patientensicherheit gefährdet werden.

Beispiele sind:

- **Katalogdaten / Terminologien**
  ICD-10-Diagnosekatalog, OPS/Leistungskatalog, SNOMED CT
- **Laborparameter**
  Grenzwerte und Verrechnungsparameter
- **Formular- und Dokumentationskonfigurationen**
  Entlassungsbriefe, Textvorlagen, Pflichtfelder, Auswahllisten und dynamische Eingabefelder
- **Klinische Regeln**
  Arzneimittelinteraktionsprüfungen und Hinweise bei kritischen Laborwerten
- **Scores / Assessments**
  NEWS2, Glasgow Coma Scale (GCS), Braden-Score
- **Referenzwerte**
  Alters- und geschlechtsspezifische Normwerte sowie therapeutische Zielbereiche
- **Behandlungspfade und Entscheidungsregeln**
  Sepsis-Behandlungspfad, Schlaganfallpfad und Thromboseprophylaxe-Entscheidungsregel
- **Interoperabilitäts-Mappings**
  Zuordnung lokaler Laborkodes zu LOINC und lokaler Diagnoseschlüssel zu ICD-10

Die Integrität und Verfügbarkeit dieser kritischer Daten werden damit zu Bestandteilen der Informationssicherheit. Entscheidend ist damit nicht allein die Art der Daten, sondern die Frage:

> Welche Auswirkungen hat es auf den Krankenhausbetrieb, wenn Daten falsch, manipuliert oder nicht verfügbar sind?

© All rights reserved - Stand: Oktober 2026

Die drei Schutzziele

Schutzziele für Bearbeitungsprozesse kritischer Daten

Für kritische Datenbearbeitungsprozesse sind insbesondere folgende drei Schutzziele relevant.

INTEGRITÄT

Integrität bedeutet, dass Informationen korrekt und vollständig sind und nicht unautorisiert oder unbemerkt verändert werden. Für Datenbearbeitungsprozesse ist dies das zentrale Schutzziel. Ein Krankenhaus muss insbesondere Risiken berücksichtigen, die entstehen durch:

- fehlerhafte manuelle Änderungen,
- Fehler durch Brüche bei manuellen und automatischen Änderungen,
- unberechtigte Änderungen,
- fehlerhafte Massenimporte,
- fehlerhafte Schnittstellen,
- technische Fehler,
- Manipulation,
- nicht nachvollziehbare Änderungen.

VERTRAULICHKEIT

Auch wenn keine Patientendaten verarbeitet werden, können betriebliche Daten einen erheblichen Schutzbedarf besitzen.

Entsprechend müssen auch bei diesen Daten Zugriff und Offenlegung risikoadäquat kontrolliert werden. Adäquate Berechtigungs- und Rollensysteme sollen den Personenkreis, der mit kritischen Daten arbeiten darf, nach dem least-to-know Prinzip minimieren.

VERFÜGBARKEIT

Kritische Informationen müssen verfügbar sein, wenn die darauf angewiesenen Prozesse sie benötigen. Dies betrifft sowohl die Anwendung selbst als auch die darin enthaltenen Daten. Relevante Fragestellungen sind beispielsweise:

- Wie lange darf das System ausfallen?
- Wie aktuell müssen die Daten sein?
- Wie schnell kann ein Datenbestand wiederhergestellt werden?
- Welche Datenverluste sind tolerierbar?
- Gibt es einen Notbetrieb?
- Können fehlerhafte Änderungen zurückgesetzt werden?

Daraus ergibt sich unter anderem die Notwendigkeit, kritische Daten entsprechend ihrem Schutzbedarf zu sichern, ihre Wiederherstellung zu ermöglichen und geeignete Versionierungs- oder Rücksetzmechanismen vorzusehen. Diese Maßnahmen unterstützen Disaster Wiederherstellung und Business Continuity.

© All rights reserved - Stand: Oktober 2026

Regulatorischer Rahmen

Rechtliche Anforderungen in Deutschland und Österreich

Die Anforderungen an den Schutz kritischer Daten im Krankenhaus ergeben sich aus gesetzlichen Vorgaben, risikobasierten Sicherheitsmaßnahmen und bewährten Praktiken. Diese drei Ebenen sind voneinander zu unterscheiden, da nicht jede sinnvolle Schutzmaßnahme unmittelbar gesetzlich vorgeschrieben ist.

1. Gesetzliche Anforderungen

Gesetzliche Vorgaben definieren verbindliche Pflichten zum Schutz kritischer Daten. In Deutschland sind insbesondere das BSIG und die NIS2-Anforderungen relevant, in Österreich das NISG 2026. Der B3S Krankenhaus konkretisiert branchenspezifische Anforderungen für Krankenhäuser in Deutschland.

2. Risikobasierte Maßnahmen

Aus den gesetzlichen Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit ergeben sich konkrete Sicherheitsmaßnahmen. Welche Kontrollen erforderlich sind, richtet sich nach dem Schutzbedarf der Daten und den Risiken für die Krankenhausprozesse.

3. Bewährte Praktiken

Ergänzende Best-Practice-Maßnahmen unterstützen die sichere und effiziente Umsetzung. Sie können über gesetzliche Mindestanforderungen hinausgehen und helfen, den Schutz kritischer Daten nachhaltig zu verbessern.



© All rights reserved - Stand: Oktober 2026

Deutschland: BSIG / NIS2

Das BSIG bildet den gesetzlichen Rahmen für das Cyber-Risikomanagement besonders wichtiger und wichtiger Einrichtungen. § 30 BSIG verlangt geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der für die Dienste verwendeten IT-Systeme, Komponenten und Prozesse zu vermeiden und die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Die Umsetzung dieser Verpflichtung muss dokumentiert werden. Für kritische Daten gemäß Definition ergeben sich daraus folgende Anforderungen.

Datenbearbeitung

Das BSIG verlangt Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen, Komponenten und Prozessen sowie ein Schwachstellenmanagement. Ein bestimmtes Verfahren für Änderungen einzelner Informationswerte – beispielsweise Vier-Augen-Freigabe oder verpflichtende Versionierung jeder Konfigurationsänderung – schreibt § 30 dagegen nicht vor. Solche Verfahren können aufgrund der Risikoanalyse erforderlich oder sinnvoll sein, sind aber keine generelle gesetzliche Einzelanforderung.

Zugriff

Hier ist das BSIG deutlich konkreter. Der gesetzliche Mindestkatalog verlangt Konzepte für Personalsicherheit und Zugriffskontrolle. Hinzu kommt die Verwendung von Multi-Faktor-Authentifizierung oder kontinuierlicher Authentifizierung sowie gesicherter Kommunikation. Damit ist ein organisatorisch geregeltes Zugriffsmanagement auf kritische Daten unmittelbar gefordert. Nicht vorgeschrieben ist dagegen eine bestimmte technische Umsetzung. Auch ein bestimmtes „Least-Privilege“-Modell wird nicht technisch vorgegeben.

Protokollierung

Eine generelle Verpflichtung, jede Änderung oder jeden Zugriff auf kritische Daten zu protokollieren, enthält § 30 BSIG nicht. Aus der Anforderung der Zugriffskontrolle und deren Nachweis ist eine Protokollierung der Zugriffe auf kritische Daten (Änderung, Kontrolle und Freigabe) aber ableitbar. Für Betreiber kritischer Anlagen kommt jedoch § 31 BSIG hinzu. Für die kritische Anlage maßgeblichen Systeme, Komponenten und Prozesse müssen Systeme zur Angriffserkennung eingesetzt werden, die geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Logging und Monitoring erhalten damit für Krankenhäuser erheblich größere Bedeutung. Trotzdem folgt daraus nicht automatisch eine Pflicht, jede einzelne fachliche Datenänderung revisionssicher zu protokollieren.

Quellenangabe: https://www.gesetze-im-internet.de/bsig_2025/

© All rights reserved - Stand: Oktober 2026

Deutschland: B3S Krankenhaus

Der B3S Krankenhaus nimmt für die vorliegende Fragestellung eine besondere Stellung ein und ist die konkreteste Grundlage für den organisatorischen Lebenszyklus wichtiger Informationen. Er ist kein eigenständiges Gesetz. § 391 Abs. 4 SGB V sieht jedoch ausdrücklich vor, dass Krankenhäuser ihre gesetzlichen Sicherheitsverpflichtungen insbesondere durch Anwendung eines vom BSI als geeignet festgestellten branchenspezifischen Sicherheitsstandards erfüllen können. Der B3S ist deshalb für die konkrete Organisation des Lebenszyklus kritischer Informationen wesentlich detaillierter als § 391 SGB V oder § 30 BSIG.

Datenbearbeitung

Für sicherheitsrelevante Änderungen bestehen geregelte Änderungs- und Freigabeprozesse. Änderungen, die Auswirkungen auf kritische Informationswerte bzw. deren Schutz haben können, müssen in die Risikobetrachtung einbezogen werden. Damit geht der B3S wesentlich weiter als § 30 BSIG. Für kritische Änderungen muss organisatorisch nachvollziehbar sein, was geändert wird, welches Risiko entsteht, wer die Änderung verantwortet bzw. freigibt, und wie mit Notfalländerungen umgegangen wird.

Zugriff

Der Zugang zu Informationswerten muss entsprechend ihrer Kritikalität geregelt werden. Dazu gehören organisatorische Vorgaben zur Vergabe und Entziehung von Zugriffsrechten sowie besondere Anforderungen für administrative Zugänge. Damit ist ein geregelter Berechtigungslebenszyklus erforderlich. Die konkrete technische Implementierung bleibt offen.

Protokollierung

Der B3S verlangt ein Protokollierungs- und Auswertungskonzept. Sicherheitsrelevante Ereignisse müssen in einem Umfang erfasst werden, der eine angemessene Überwachung und Auswertung ermöglicht. Für besonders schutzbedürftige Systeme bestehen erhöhte Anforderungen, insbesondere hinsichtlich administrativer Aktivitäten und des Schutzes relevanter Protokolldaten vor nachträglicher Manipulation. Damit ist Logging im B3S wesentlich konkreter geregelt als im BSIG selbst. Aus der Anforderung der Zugriffskontrolle und deren Nachweis ist eine Protokollierung der Zugriffe auf kritische Daten (Änderung, Kontrolle und Freigabe) ableitbar.

Quellenangabe:
https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/

© All rights reserved - Stand: Oktober 2026

Österreich: NISG 2026

Das österreichische NISG 2026 verfolgt strukturell einen ähnlichen Ansatz wie das deutsche BSIG. § 32 verpflichtet wesentliche und wichtige Einrichtungen zu geeigneten und verhältnismäßigen technischen, operativen und organisatorischen Risikomanagementmaßnahmen. Sie müssen die Sicherheitsrisiken für die zum Betrieb bzw. zur Erbringung der Dienste verwendeten Netz- und Informationssysteme reduzieren und die Auswirkungen von Cybersicherheitsvorfällen möglichst gering halten. Das Sicherheitsniveau muss dem bestehenden Risiko entsprechen.

Datenbearbeitung

Das NISG verlangt Sicherheitsmaßnahmen bei Beschaffung, Entwicklung und Wartung sowie Schwachstellenmanagement. Ein konkretes Freigabeverfahren für jede Änderung eines wichtigen Informationswertes schreibt es dagegen nicht vor. Standardisierte Bearbeitungs-, Kontroll- und Freigabeprozesse sind je nach Risiko aber geeignete Maßnahmen, um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Zugriff

Zugriffskontrolle, Personalsicherheit und Asset Management gehören zum gesetzlichen Maßnahmenkatalog. Hinzu kommen Multi-Faktor- bzw. kontinuierliche Authentifizierung und Anforderungen an sichere Kommunikation. Damit muss der Zugriff auf kritische Ressourcen organisatorisch kontrolliert werden; ein bestimmtes technisches Rollen- oder Berechtigungsmodell ist nicht vorgeschrieben.

Protokollierung

Eine allgemeine gesetzliche Verpflichtung, sämtliche Zugriffe und Änderungen wichtiger Daten zu protokollieren, besteht nicht. Logging und Monitoring können aber notwendig sein, um Sicherheitsvorfälle zu erkennen, zu untersuchen und die Wirksamkeit der Sicherheitsmaßnahmen nachweisen zu können. Um die Einhaltung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit nachweisen zu können, ist eine Protokollierung kritischer Datenprozesse ableitbar.

Quellenangabe:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20013065

© All rights reserved - Stand: Oktober 2026

Vier Schutzstufen

Anforderungen an sichere Datenbearbeitungsprozesse im Krankenhaus

Nicht jede Datenänderung erfordert dasselbe Sicherheitsniveau. Entscheidend ist die Kritikalität der Daten. Ein risikobasierter Ansatz kann beispielsweise vier Schutzstufen unterscheiden. Die folgende Einteilung dient als beispielhaftes Schutzstufenmodell.

Standard

Mögliche Auswirkungen fehlerhafter Daten:
geringe betriebliche Auswirkungen

Kontrollniveau:
Basiskontrollen

Erhöht

Mögliche Auswirkungen fehlerhafter Daten:
relevante Prozessbeeinträchtigung

Kontrollniveau:
zusätzliche Validierung und Nachvollziehbarkeit

Kritisch

Mögliche Auswirkungen fehlerhafter Daten:
erhebliche Betriebsbeeinträchtigung

Kontrollniveau:
Freigabe, Audit und Wiederherstellung

Hochkritisch

Mögliche Auswirkungen fehlerhafter Daten:
Gefährdung kritischer Krankenhausfunktionen

Kontrollniveau:
besonders strenge präventive Kontrollen



© All rights reserved - Stand: Oktober 2026

Datenhaltung und Least-to-know-Prinzip

Datenhaltung

Kritische Daten sollten möglichst zentral als „Single Source of Truth“, vorzugsweise in Datenbanken, gehalten werden. Definierte Datenmodelle können zusätzlich die Datenqualität sicherstellen.

Verantwortlichkeit

Für kritische Daten müssen Verantwortlichkeiten eindeutig geregelt sein, insbesondere für Datenverantwortung, Pflege, Freigabe, Schnittstellen, Datenqualität und Sicherheitsvorfälle. Technische Berechtigungen sollten diese Rollen abbilden.

Zugriffskontrolle

Das Least-to-know-Prinzip sollte auch auf die Datenbearbeitung angewendet werden. Nicht jeder Benutzer, der Daten lesen darf, muss diese ändern dürfen. Ebenso sollte zwischen unterschiedlichen Änderungsrechten unterschieden werden können. Ein typisches Berechtigungsmodell könnte beispielsweise folgende Berechtigungsstufen umfassen:



Besonders privilegierte Rollen sollten zusätzlichen Sicherheitsmaßnahmen unterliegen.



© All rights reserved - Stand: Oktober 2026

Kontrollierte Prozesse

Validierung

Fehlerhafte Daten sollten möglichst vor ihrer produktiven Nutzung verhindert werden. Dazu dienen unter anderem Pflichtfelder, Datentyp- und Wertebereichsprüfungen, Referenzintegrität, Eindeutigkeits- und Plausibilitätsprüfungen sowie konfigurierbare Business Rules.

Kontrollierte Freigabe

Freigabeprozesse sollten sich an der Kritikalität orientieren und unterschiedliche Kontrollstufen, etwa nach dem Zwei-, Vier- oder Sechs-Augen-Prinzip, ermöglichen. Bearbeitung, Kontrolle und Freigabe sollten getrennt werden können. Für zeitkritische Änderungen sollte ein dokumentierter Emergency-Change-Prozess mit nachgelagertem Review bestehen.

Nachvollziehbarkeit

Änderungen kritischer Daten müssen nachvollziehbar sein. Ein Audit Trail sollte insbesondere Identität, Zeitpunkt, Datenobjekt, Aktion, Alt- und Neuwert, Änderungsgrund, Freigabe und Änderungskanal dokumentieren. Dies gilt für manuelle Änderungen ebenso wie für APIs, Importe und Batchprozesse.



Schnittstellen

Massenänderungen und Datenimporte

Bulk-Änderungen besitzen aufgrund ihrer Reichweite ein erhöhtes Risiko. Für kritische Daten sollten daher kontrollierte Importprozesse mit Preview/Dry-Run, Validierung, Fehlerberichten, Benutzerzuordnung, Transaktionssicherheit und Rollbackmöglichkeiten vorgesehen werden.

Schnittstellen

Automatisierte Änderungen sind hinsichtlich der Datenintegrität ebenso zu kontrollieren wie manuelle Eingriffe. Schreibende Schnittstellen benötigen insbesondere Authentifizierung, Autorisierung, Validierung, Logging, Fehlerbehandlung und Monitoring. Grundsätzlich muss jeder Schreibpfad auf kritische Daten kontrollierbar und nachvollziehbar sein.

© All rights reserved - Stand: Oktober 2026

Anforderungen an Software

Software für die Bearbeitung kritischer Daten sollte insbesondere folgende Funktionen unterstützen:

Identity & Access Management:
Rollen- und Rechtekonzept, Least Privilege, SSO/MFA und kontrollierte Service Accounts.

Audit Trail:
manipulationsgeschützte Nachvollziehbarkeit kritischer Änderungen.

Freigabeworkflows:
konfigurierbare Kontroll- und Freigabestufen entsprechend der Risikoklasse.

Versionierung und Wiederherstellung:
Historisierung, Vergleich, Rollback und Wiederherstellung früherer Datenstände.

Sichere Schnittstellen und Importe:
Authentifizierung, Autorisierung, Validierung, Logging und Fehlerbehandlung.

Diese Funktionen unterstützen die risikogerechte Umsetzung zentraler Anforderungen an Zugriffsschutz, Datenintegrität und Nachvollziehbarkeit.



© All rights reserved - Stand: Oktober 2026

Fazit und Ausblick

Kritische Datenbearbeitung als kontrollierter Prozess

Regulatorische Anforderungen an die Informationssicherheit erhöhen auch die Anforderungen an die Datenbearbeitung in Krankenhäusern. Für kritische Daten werden Integrität, Verfügbarkeit und Vertraulichkeit zu Bestandteilen des Compliance- und Risikomanagements.



Zentrale Schlussaussage

Datenbearbeitung ist damit nicht nur eine administrative Funktion, sondern ein kontrollierter Prozess. Kritische Daten müssen über ihren gesamten Änderungslebenszyklus autorisiert, validiert, nachvollziehbar und wiederherstellbar verwaltet werden.

Daraus ergibt sich kein einzelnes regulatorisch vorgeschriebenes Softwarefeature, sondern ein umfassendes Zielbild für sichere Datenbearbeitung. Die eingesetzte Software und ihr Anbieter müssen dabei ebenfalls in das Sicherheits- und Lieferkettenmanagement des Krankenhauses eingebunden sein.

Rechtlicher Hinweis

Dieses Whitepaper dient der allgemeinen fachlichen Information und stellt keine Rechtsberatung dar. Die dargestellten regulatorischen Anforderungen entsprechen dem Informationsstand Oktober 2026. Die konkrete Anwendbarkeit hängt insbesondere von Größe, Einstufung, Trägerschaft, technischer Architektur und Kritikalität der jeweiligen Einrichtung ab. Die geltenden rechtlichen Anforderungen und deren Umsetzung sind für das jeweilige Krankenhaus und den konkreten Einsatzfall individuell zu prüfen. Trotz sorgfältiger Erstellung wird keine Gewähr für die Vollständigkeit und Aktualität der Inhalte übernommen.

© All rights reserved - Stand: Oktober 2026

BOI BETTER ORGANIZED INFORMATION

IHR SPEZIALIST FÜR BESSER ORGANISIERTE INFORMATION

BOI Software Entwicklung und Vertrieb GmbH

Über 45 Jahre Erfolg und Innovation.
Ihr Experte für Tabellenmanagement.

Wir entwickeln innovative Softwarelösungen für revisionssichere Datenbearbeitung sowie hochperformanten Datenzugriff, um die Verwaltung Ihrer kritischen Daten besser zu organisieren.

ISO/IEC 27001 zertifiziert. Sicher. Zukunftsorientiert.



OFFICE GRAZ

| Friedrichgasse 30/1, 8010 Graz, Austria

OFFICE LINZ

| Spazgasse 4, 4040 Linz, Austria

KONTAKT

| +43 (0) 732 736423 - 0
| office@boi.at
| www.boi.at



IHR ANSPRECHPARTNER FÜR DATEN-MANAGEMENT

Dr. Frank Sinner
Geschäftsführung

Telefon: +43 (0) 732 736 423 - 0
Mobil: +43 664 147 71 68
E-Mail: frank.sinner@boi.at