Benjamin Tobies
pflegedozi.de
Spierling 9
25917 Stadum
info@pflegedozi.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat Cyber-Sicherheit im Gesundheitswesen
Postfach 20 03 63
53133 Bonn
primaersystem@bsi.bund.de

Stadum, 31. Mai 2026

Stellungnahme zur Konsultation der Handlungsempfehlungen zur Verbesserung der IT-Sicherheit in ambulanten Pflegediensten (DiPS)

Konsultationsfassung des BSI vom 13.02.2026 — Frist 17.06.2026

1. Einleitung und Perspektive des Verfassers

Der Verfasser dieser Stellungnahme arbeitet seit 1999 in der pflegerischen und präklinischen Versorgung — von 1999 bis 2004 als Rettungssanitäter, seit 2007 nach Vollzeit-Umschulung als examinierter Altenpfleger. Stationen seines weiteren Berufswegs waren die ambulante und stationäre Altenpflege, Tätigkeiten als Wundpfleger und Qualitätsbeauftragter, ergänzt um Erfahrung in Pflegedienstleitungs-Funktionen. Bis heute ergänzt wird die pflegerische Tätigkeit durch die Rolle als Praxisanleiter für Auszubildende in der Pflegeausbildung. Hauptberuflich tätig ist er als freiberuflicher Dozent für Pflegeeinrichtungen — Live-Fortbildungen, Schulungsmodule und QM-Werke aus eigener Praxis.
Aus dieser Praxis heraus hat der Verfasser seit Herbst 2025 ein Open-Source-Pflegedokumentations-Ökosystem entwickelt: PflegeDoku Pro, bestehend aus sieben eigenständigen, unter AGPLv3 lizenzierten Modulen für Dokumentation, Abrechnung, Dienstplanung, Lohn- und Gehaltsabrechnung, Zeiterfassung, ein Analyse- und Briefingmodul (Intelligence) sowie die zentrale Systemverwaltung. Das Ökosystem ist als Komplettsystem mit lokaler Datenhaltung und ohne Cloud-Komponente angelegt. Ein internes Audit gegen den BSI-DiPS-Befundkatalog wurde vom Verfasser zwischen dem 25. April und dem 6. Mai 2026 selbst durchgeführt; die acht Sofortmaßnahmen aus dem dabei dokumentierten Befundkatalog wurden bis zur ausgelieferten Version 0.9.0 vom 20. Mai 2026 umgesetzt. Die ausgelieferte Version wird derzeit in einem strukturierten Übergabeverfahren an erste interessierte Einrichtungen weitergegeben. Anhang B dieser Stellungnahme dokumentiert das System und die Audit-Spur im Detail.
Aus dieser Doppelrolle ergibt sich die Perspektive der vorliegenden Stellungnahme: Sie liest die DiPS-Handlungsempfehlungen einerseits mit dem Blick eines Anwenders und Pflegelehrers, der die Umsetzungs-Last in kleinen ambulanten Diensten und in der Ausbildung kennt — und andererseits mit dem Blick eines Entwicklers, der die gleichen Schwachstellen-Befunde, die der DiPS-Pentest dokumentiert hat, im eigenen Code adressiert hat und daraus einschätzen kann, welche Maßnahmen welche Form von Wirkung entfalten.

Diese Doppelperspektive fehlt typischerweise in den großen Verbandsstellungnahmen — die Anwender-Perspektive ist dort gut vertreten, die Hersteller- und Architektur-Perspektive aus dem deutschen Pflege-IT-Markt jedoch kaum. Die hier vorliegende Stellungnahme versucht, beides zusammenzuführen.

2. Allgemeine Würdigung

Die vom BSI vorgelegte Studie DiPS (Abschlussbericht und Handlungsempfehlungen vom 13.02.2026) ist als Ganzes anzuerkennen. Sie liefert den ersten systematischen, öffentlich verfügbaren Penetrationstest-Befund zu Pflegedokumentationssystemen im deutschsprachigen Raum und schließt damit eine Lücke, die für die Pflege-IT — anders als für die Praxisverwaltungssysteme (SiPra), Krankenhausinformationssysteme (SiKIS) und perspektivisch die Telematikinfrastruktur — bislang strukturell offen war. Die Auswahl von drei marktrelevanten Pflegedokumentationssystemen, die Erfassung in zwölf Schwachstellen-Klassen und die Veröffentlichung der Empfehlungen in einem öffentlichen Konsultationsverfahren entsprechen einem belastbaren Wissenschafts- und Verwaltungsstandard.
Ausdrücklich anerkannt sei das Coordinated-Vulnerability-Disclosure-Verfahren, das das BSI mit den getesteten Herstellern durchgeführt hat. Die schriftlich dokumentierte Abstimmung über das Veröffentlichungsdatum ist eine Disziplin, die in der Sicherheitsforschung nicht selbstverständlich ist und einen konstruktiven Umgang zwischen Aufsicht, Herstellern und Öffentlichkeit fördert. Ebenso zu begrüßen ist, dass die Handlungsempfehlungen vor ihrer Endfassung in eine öffentliche Konsultation gegeben werden — eine Form der Verfahrens-Offenheit, die in der deutschen IT-Sicherheits-Aufsicht keineswegs Standard ist.
Auf dieser grundsätzlich anerkennenden Position bauen die folgenden Kapitel auf. Sie adressieren zwei strukturelle Lücken, die sich aus der Doppelperspektive des Verfassers (Kapitel 1) ergeben und in den großen Verbandsstellungnahmen aus Sicht des Verfassers bislang unterbelichtet sind: Erstens die Adressaten-Asymmetrie zwischen den DiPS-Empfehlungen (an die betreibenden Pflegedienste gerichtet) und den SiPra-Empfehlungen (an die Hersteller gerichtet) — eine Setzung, die für eine ganze Befundklasse die Umsetzbarkeit aus Sicht der adressierten Pflegedienste strukturell blockiert (Kapitel 3.1). Zweitens das im Empfehlungstext nicht reflektierte Marktbild proprietärer, vom Hersteller gepflegter Software, das eine alternative Architekturoption — Open-Source-Software mit lokaler Datenhaltung — als gleichberechtigte Variante ausklammert (Kapitel 4). Beide Lücken sind in der Endfassung der Handlungsempfehlungen adressierbar; die Stellungnahme legt jeweils konkrete Empfehlungstexte vor.

3. Strukturelle Anmerkungen

3.1 Adressaten-Asymmetrie zwischen SiPra und DiPS

Das BSI hat im Februar 2026 zwei Abschlussberichte und Handlungsempfehlungen zur IT-Sicherheit im ambulanten Gesundheitssektor vorgelegt: SiPra zu Praxisverwaltungssystemen und DiPS zu Pflegedokumentationssystemen. Beide Projekte adressieren strukturell verwandte Schwachstellen-Cluster. Die Adressaten-Kategorie der Empfehlungen ist jedoch unterschiedlich angelegt: SiPra richtet sich an die Hersteller der

Praxisverwaltungssysteme, DiPS richtet sich an die betreibenden Pflegedienste. Diese Asymmetrie ist nicht durch die Sache begründet — die Befundklassen sind in beiden Studien vergleichbar — sondern eine Setzung des jeweiligen Empfehlungs-Dokuments.
Diese Asymmetrie hat eine konkrete Folge für die Wirksamkeit der DiPS-Empfehlungen: Schwachstellen, die im Hersteller-Code entstehen, sind durch Maßnahmen der Betreibenden nicht behebbar. Das zeigt sich an mehreren der DiPS-Penetrationstest-Befunde — fehlende Server-Authentifizierung in TLS-Verbindungen, hardcodierte Zugangsdaten in Installationspaketen, dauerhaft offene Wartungszugänge der Hersteller (siehe Belege in 5.1, 5.3 und 5.5). Eine Pflegeeinrichtung kann diese Befunde nicht durch eigene Konfiguration adressieren; sie kann nur das einkaufen, was der Markt anbietet, und hoffen, dass der Hersteller die Befunde im Code adressiert. Die Adressierung über die Betreibenden ist damit für eine ganze Befundklasse strukturell wirkungslos.
Aus dieser Beobachtung folgt eine konkrete Empfehlung an das BSI: ein paralleles Hersteller-adressiertes Empfehlungsdokument für Pflegedokumentationssysteme, analog zur SiPra-Konstruktion für Praxisverwaltungssysteme. Der Deutsche Pflegerat hat in seinem Expert:innenpapier „Cybersicherheit in der pflegerischen Versorgung“ vom Juni 2025 in dieselbe Richtung argumentiert und verbindliche IT-Sicherheitsstandards für Hersteller sowie eine Zertifizierung der Produkte nach klar definierten Kriterien gefordert (siehe ausführlich 5.3 sowie Anhang C). Ein BSI-Empfehlungsdokument für Hersteller von Pflegedokumentationssystemen wäre der naheliegende Anschluss-Schritt zu dieser Forderung — und die strukturelle Voraussetzung dafür, dass die DiPS-Empfehlungen an die Betreibenden überhaupt umsetzbar werden.

3.2 Realismus für kleine Adressaten

Ambulante Pflegedienste sind als Adressatengruppe deutlich heterogener, als die DiPS-Empfehlungen es voraussetzen. Die Bandbreite reicht vom Kleinstdienst mit drei bis fünf Mitarbeitenden in einer ländlichen Region bis zu Trägerstrukturen mit über 200 Mitarbeitenden und eigener IT-Abteilung. Empfehlungen, die für die obere Bandhälfte tragbar sind — zentrales Mobile Device Management (MDM), professionelle Netzwerksegmentierung, ein vollständig dokumentiertes Information Security Management System (ISMS) — sind für die untere Bandhälfte ökonomisch und personell nicht leistbar. Das ist keine Frage des guten Willens, sondern der verfügbaren Ressourcen: Lizenzkosten und Personal-Slot für IT-Sicherheits-Compliance stehen in Kleinstdiensten nicht im benötigten Umfang zur Verfügung.
Das DiPS-Dokument erkennt diese Differenz an mehreren Stellen — bei der Netzwerksegmentierung im Hinweis, dass sie für kleinere Betreibende meist nicht sinnvoll ist (wörtliches Zitat in 5.2), bei der MDM-Empfehlung im Hinweis auf die ökonomische Grenze für kleinere Dienste (wörtliches Zitat in 5.4), und beim Risikomanagement im Hinweis, dass ein vollständiges ISMS für kleine Einrichtungen nicht immer sinnvoll ist (wörtliches Zitat in 5.6). Die Differenzierung ist also bereits angelegt — sie ist jedoch nicht in eine systematische Empfehlungs-Struktur überführt. Eine Betreiberin liest das Dokument linear und stößt erst beim jeweiligen Kapitel auf den Hinweis, dass diese Empfehlung für sie gegebenenfalls nicht zutrifft. Eine vorgelagerte Empfehlungs-Schichtung würde diese Such-Last reduzieren.
Diese Stellungnahme schlägt konkret gestaffelte Empfehlungs-Profile nach Dienstgröße vor — als pragmatische Faustregel in Anlehnung an typische Personal-Strukturen ambulanter Pflegedienste etwa in drei Klassen: bis fünf

Mitarbeitende (Kleinstdienst), sechs bis 25 (mittelgroßer Dienst) und über 25 (großer Dienst mit eigenen Verwaltungsstrukturen). Für die unterste Klasse sollte ein reduziertes Mindest-Profil definiert sein, das nur die Maßnahmen verlangt, die ohne externe IT-Unterstützung umsetzbar sind. Für die mittlere Klasse kommt der in 5.6 vorgeschlagene Förderpfad als Verstärkungs-Strecke hinzu — er macht Empfehlungen umsetzbar, die ohne Förderung an der wirtschaftlichen Grenze der Adressaten scheitern. Für die obere Klasse können die vollständigen DiPS-Empfehlungen als Profil tragen. Die Schwellen sind nicht als starre Grenzen gemeint, sondern als Orientierungs-Korridor; eine externe statistische Stratifikation — etwa aus Pflegekassen-Daten — könnte sie präzisieren.

4. Die fehlende Architekturoption: Open Source und lokale Datenhaltung

4.1 Was die Empfehlungen voraussetzen, ohne es zu nennen

Sowohl die Schwachstellen-Befunde des DiPS-Abschlussberichts als auch die daraus abgeleiteten Handlungsempfehlungen setzen ein bestimmtes Marktbild voraus: proprietäre Software, vom Hersteller entwickelt und gepflegt, ausgeliefert entweder als Client-Server-Installation beim Betreiber oder als Cloud-Dienst beim Hersteller. Diese Annahme ist nicht falsch — sie beschreibt den heutigen Pflege-IT-Markt zutreffend — aber sie ist eine Annahme, keine technische Notwendigkeit. Sie wird im Dokument an keiner Stelle als Annahme markiert.

Zwei Stellen machen das Marktbild im Empfehlungstext sichtbar. Erstens in BSI 4.4: Cloud-Betrieb wird als die Strecke mit der geringeren Konfigurations-Verantwortung der Betreibenden dargestellt — eine Empfehlungs-Tendenz, die ein bestimmtes Hersteller-Betreiber-Verhältnis voraussetzt (wörtliches Zitat und Auseinandersetzung in 5.9). Zweitens in BSI 3.5: „Die Hersteller von Pflegedokumentationssystemen tragen durch die Entwicklung sicherer Software zur IT-Sicherheit in den ambulanten Pflegediensten bei. Neben der Software bieten die Hersteller in der Regel auch eine Dokumentation dazu an. In dieser sind oft sicherheitsrelevante Konfigurationen beschrieben.“ Sicherheitsrelevante Konfiguration ist hier als Hersteller-Dokumentations-Strecke gedacht: Der Betreibende erkundigt sich beim Hersteller, der Hersteller stellt das Dokument bereit, der Betreibende setzt um.

In beiden Fällen ist nicht das Gesagte das Problem, sondern das Nicht-Gesagte. Eine alternative Architektur — Open Source, lokale Datenhaltung, öffentlich einsehbarer Quellcode und Audit-Spur — verlangt die genannten Strecken nicht. Sicherheitsrelevante Konfiguration ist dort im Quellcode, in den CHANGELOG-Dateien und in der Release-Spur dokumentiert (siehe ausführlich 5.5); die Verfügbarkeits- und Datenschutz-Verantwortung verlagert sich nicht an einen Cloud-Anbieter, sondern bleibt beim Betreibenden (siehe 5.9). Die DiPS-Handlungsempfehlungen nehmen diese Architekturoption nicht als gleichberechtigte Variante auf. Kapitel 4.2 bis 4.4 dieser Stellungnahme legen dar, was sich strukturell ändert, wenn sie aufgenommen wird.

4.2 Was sich strukturell ändert mit Open-Source-Architektur

Eine Open-Source-Architektur mit lokaler Datenhaltung verändert die Sicherheits-Topologie eines Pflegedokumentationssystems an vier strukturellen Stellen — nicht als zusätzliche Sicherheits-Maßnahme on top, sondern als

anderer Ausgangspunkt.
Erstens: Auditierbarkeit ist nicht ans Vertrauen in den Hersteller gebunden. Bei proprietärer Software steht eine Betreiberin vor der Frage, ob die Sicherheitszusagen des Herstellers tatsächlich im Code stehen. Sie kann es nicht prüfen. Bei Open-Source-Software unter einer Copyleft-Lizenz wie AGPLv3 ist der Quellcode öffentlich; jeder beauftragte IT-Dienstleister kann jede Sicherheitszusage gegen den Code prüfen. Das in Anhang B beschriebene Selbst-Audit gegen den BSI-DiPS-Befundkatalog ist Beispiel für diese Prüfbarkeit: Es konnte vom Verfasser durchgeführt werden, weil der gesamte Code zugänglich war — eine Voraussetzung, die bei proprietärer Software strukturell nicht gegeben ist.
Zweitens: Update-Mechanismen sind öffentlich nachvollziehbar. Der DiPS-Abschlussbericht hat in den Penetrationstests dokumentiert, dass Update-Strecken bei den getesteten Systemen einer der Schwachpunkt-Cluster sind. Wenn der Update-Mechanismus selbst Quellcode ist, der öffentlich liegt, kann sein Verhalten gegen die Erwartung geprüft werden — kein Update kommt aus einer Black Box. Die modulweisen CHANGELOG-Dateien jeder Auslieferung dokumentieren, was sich geändert hat, mit Commit-Hash und Befund-Bezug (siehe Anhang B.5a für die M1-Maßnahmenspur als Beispiel).
Drittens: Lokale, offline-fähige Installation hebt die Angriffsfläche „Internet-erreichbarer Server“ strukturell auf. Was nicht aus dem Internet erreichbar ist, kann nicht aus dem Internet angegriffen werden. Das ist keine triviale Aussage, sondern die direkteste Antwort auf einen großen Teil der im DiPS-Pentest gefundenen Befunde — von TLS-Konfigurationsfehlern bis zu unauthentisierten Endpunkten (siehe ausführlich 5.1 und 5.2). Eine Architektur, in der die Modul-zu-Modul-Kommunikation per Default auf 127.0.0.1 gebunden ist und ein LAN- oder Internet-Exposing eine explizite Konfiguration verlangt, verschiebt nicht das Problem, sondern entfernt eine ganze Befundklasse vor ihrem Eintreten.
Viertens: Es entsteht kein Lieferanten-Lock-in. Bei proprietärer Cloud-Software liegen Patientendaten in proprietären Formaten beim Anbieter; ein Wechsel zu einem anderen Produkt erfordert Export-Schnittstellen, die häufig fehlen oder eingeschränkt sind. Bei Open-Source-Software unter AGPLv3 sind sowohl Daten als auch Code beim Betreibenden; ein Anbieterwechsel ist möglich, ohne dass die Datenhoheit den Betreibenden verlässt. Im KRITIS- und NIS2-Kontext (Anhang C) ist dieser Punkt nicht nur eine wirtschaftliche, sondern eine Resilienz-Frage: Wenn ein Cloud-Anbieter ausfällt — durch Cyberangriff, Insolvenz, geopolitische Verwerfungen oder regulatorische Eingriffe —, fällt nicht ein Pflegedienst aus, sondern alle seine Kunden gleichzeitig. Lokale Installation pro Pflegedienst macht den Ausfall zur Einzel-Frage, nicht zur Sektor-Frage.

4.3 Warum Pflege-spezifisch

Die in 4.2 genannten Eigenschaften gelten allgemein für sicherheitsrelevante Software; der Pflegekontext schärft sie. Pflege verarbeitet hochsensible Daten — Diagnosen, Medikationen, Pflegegrade, Vitalwerte, oft auch psychiatrische und endbegleitende Verläufe — unter den knappsten Personal- und Zeitressourcen eines durchregulierten Sektors. Das ist die für IT-Sicherheits-Compliance schlechteste denkbare Kombination: maximaler Schutzbedarf bei minimalem Personal-Slot für die Umsetzung der dazu nötigen Maßnahmen. Eine Architektur, die strukturell weniger angreifbar ist, ist hier mehr wert als eine, die per Checkliste sicher konfiguriert werden müsste — weil das Personal für die Checklisten-Pflege schlicht fehlt.
Diese Lücke ist nicht durch Aufrufe an die Betreibenden zu schließen, sondern durch zwei strukturelle Schritte: einen Förderpfad, der Sicherheits-Investitionen

über die Hersteller bündelt statt über den einzelnen Dienst (ausführlich in 5.6), und eine Architekturoption, die das Sicherheits-Niveau im Auslieferungszustand hochsetzt, statt es in die Konfigurations-Verantwortung der Betreibenden zu verlagern. Beides zusammen ändert das Verhältnis von Aufwand zu Schutz für die genannten kleinen und mittleren Pflegedienste.
Ein letzter Punkt ist lizenz-spezifisch. Open Source ist nicht gleich Open Source. Permissive Lizenzen (MIT, BSD, Apache) erlauben, dass Modifikationen am Code nicht zurückfließen müssen — ein Hersteller kann ein quelloffenes Pflegedokumentationssystem nehmen, eine Cloud-Variante daraus bauen und die Änderungen für sich behalten. Die AGPLv3-Lizenz schließt diese Strecke: Wer Modifikationen über ein Netzwerk anbietet, muss den modifizierten Quellcode öffentlich machen. Das ist der entscheidende Unterschied zwischen „prüfbar im Auslieferungszustand“ und „prüfbar auch nach jeder Hersteller-Modifikation“. Für eine Branche mit Schutzbedarf nach Art. 9 DSGVO ist das nicht eine Lizenz-Feinheit, sondern die Voraussetzung dafür, dass Auditierbarkeit dauerhaft trägt.

4.4 Beispiel-Implementierung

Die in 4.2 und 4.3 dargestellte Architekturoption ist keine theoretische Position. Sie liegt seit Mai 2026 als ausgeliefertes Komplettsystem vor — entwickelt vom Verfasser dieser Stellungnahme, in Deutschland, unter AGPLv3.
PflegeDoku Pro ist ein Ökosystem aus sieben eigenständigen Fachprogrammen für Pflegedokumentation (SIS), Abrechnung, Dienstplanung, Mitarbeiter-Abrechnung, Zeiterfassung, analytische Auswertung sowie einen Systemassistenten für Installation, Health-Check und Backup (Modul-Übersicht in Anhang B.2). Tech-Stack: Python 3.10+ mit PyQt6 als Oberfläche, SQLite pro Programm zur Datenhaltung, Fernet-Verschlüsselung sicherheitsrelevanter Felder, REST-Kommunikation über Loopback (127.0.0.1) zwischen den Modulen. Trägersystem ist jedes übliche Linux-System (siehe Anhang B.1). Keine Cloud-Komponente. Keine öffentlich erreichbaren Endpunkte im Default-Auslieferungszustand. Alle sieben Module einheitlich unter AGPLv3.
Das Ökosystem wurde zwischen 25.04.2026 und 06.05.2026 in einem internen Selbst-Audit gegen den BSI-DiPS-Befundkatalog geprüft — 55 dokumentierte Befunde, vollständige schriftliche Audit-Spur (Anhang B.5). Acht Sofortmaßnahmen wurden zwischen 13.05. und 20.05.2026 in sieben Modul-Codebasen umgesetzt, mit Pflicht-Smoke-Tests pro Maßnahme und atomarer Commit-Spur pro Befund (Anhang B.5a). Die auditfeste Komplettsystem-Version 0.9.0 ist ausgeliefert; die finale Veröffentlichung der MDR-freien Basisversion ist im Juli 2026 vorgesehen.
Aus dieser Implementierung ergibt sich eine konkrete Empfehlung an das BSI: Open-Source-Architekturen mit lokaler Datenhaltung als gleichberechtigte Option in die Handlungsempfehlungen aufzunehmen. Bezugsrahmen für diese Empfehlung sind das Prinzip „Public Money — Public Code“ der Free Software Foundation Europe sowie der Förderansatz der Sovereign Tech Agency, beide in Anhang C belegt. Die hier beschriebene Implementierung steht für einen fachlichen Austausch zur Verfügung; der Verfasser bringt Bereitschaft zur Pilotprojekt-Beteiligung und zu Praxistests im Pflegeschulkontext ausdrücklich ein.

5. Kapitelweise Anmerkungen zu den DiPS-Handlungsempfehlungen

5.1 Zu BSI-Kapitel 3.1 (Kommunikationssicherheit)

Die in BSI 3.1 formulierte Pflicht zu Transport Layer Security („Die Vertraulichkeit und Integrität der Netzwerkkommunikation sollten durch die Verwendung sicherer und weitverbreiteter Kommunikationsprotokolle geschützt werden“, BSI 3.1.1) sowie der Verweis auf TR-02102-2 zur sicheren Konfiguration (3.1.2) und auf die saubere Authentifizierung der Kommunikationsendpunkte (3.1.3) sind sachlich vollständig und treffen den Stand der Technik präzise. Die Belege aus dem DiPS-Abschlussbericht zeigen zudem, dass diese Forderungen nicht abstrakt sind: „In mehreren Fällen authentifizieren die Anwendungen die Identität externer Server während TLS-Verbindungen nicht korrekt, wodurch sie für ‚Meddler-in-the-Middle-Angriffe‘ […] anfällig werden“ (DiPS-Abschlussbericht 4.1).
Die Adressierung der Empfehlung gilt jedoch ausschließlich der betreibenden Pflegeeinrichtung — die Mängel, die der Penetrationstest findet, entstehen jedoch im Code der Hersteller. Eine Betreiberin kann „TLS-Konfiguration gemäß Herstellervorgaben“ nur dann sinnvoll umsetzen, wenn der Hersteller die Konfiguration auch sicher ausliefert. Dies ist eine wiederkehrende Asymmetrie zwischen Hersteller- und Betreiberverantwortung, auf die diese Stellungnahme in Kapitel 3.1 grundsätzlich und in mehreren Unterpunkten von Kapitel 5 mit konkretem Empfehlungsbezug zurückkommt.
In der hier vorgestellten Implementierung verzichtet die Loopback-Architektur (Modul-zu-Modul-Kommunikation über 127.0.0.1) bewusst auf TLS, weil keine Netzwerkstrecke existiert. Sobald die Software für LAN- oder Reverse-Proxy-Betrieb konfiguriert wird, ist TLS Pflicht und im Systemassistenten als expliziter Konfigurationsschritt vorgesehen. Diese Architekturentscheidung adressiert die im Pentest gefundene Befundklasse vor ihrem Eintreten.

5.2 Zu BSI-Kapitel 3.2 (Netzwerksicherheit)

Die Differenzierung in BSI 3.2 ist realistisch: für größere Betreibende Netzwerksegmentierung als Maßnahme, für kleinere ein robustes WLAN-Passwort und der Schutz physischer Netzwerkdosen (3.2.1). Die Empfehlung in 3.2.2 — „möglichst wenige Systeme aus dem Internet erreichbar zu machen“ — und der Hinweis auf VPN als Alternative sind ebenfalls anschlussfähig. Insbesondere die Feststellung, dass „eine Netzwerksegmentierung […] meist nur für größere Netzwerke sinnvoll [ist]“ und kleinere Betreibende „häufig nicht von einer Netzwerksegmentierung [profitieren]“, vermeidet die in der Praxis verbreitete Falle, kleinen Pflegediensten Aufwand zuzumuten, der nur in mittelständischen IT-Landschaften umsetzbar ist.
Die Empfehlung setzt allerdings voraus, dass Betreibende überhaupt entscheiden können, ob ihre Software Internet-Exposition braucht. In der Praxis kommt diese Entscheidung mit dem gewählten Produkt: Cloud-Produkte verlangen sie zwangsläufig, On-Premise-Produkte können sie vermeiden. Die Produktwahl ist damit auch eine netzwerksicherheits-Entscheidung — das DiPS-Dokument macht das in 3.2 nicht explizit, in 4.4 dann aber sehr wohl (siehe hierzu 5.9).
Die hier vorgestellte Implementierung bindet seit der Sicherheits-Härtung im Mai 2026 standardmäßig auf 127.0.0.1; ein LAN-Bind erfolgt nur nach explizitem Konfigurationsschritt im Systemassistenten, eine Internet-Exposition ist nicht als unterstütztes Szenario vorgesehen. Damit ist die in BSI 3.2.2 erwünschte Minimierung der exponierten Dienste der Default-Zustand, nicht ein

Konfigurationsziel, das die betreibende Einrichtung aktiv erreichen müsste.

5.3 Zu BSI-Kapitel 3.3 (Usermanagement und Passwörter)

Die drei Empfehlungen in BSI 3.3 — regelmäßiges Audit der Nutzerkonten (3.3.1), temporäre Aktivierung von Wartungszugängen (3.3.2) sowie Passwortrichtlinie und MFA bei Internet-Erreichbarkeit (3.3.3) — sind sachlich präzise. Die Beobachtung im DiPS-Abschlussbericht zur Wartungszugangs-Realität ist dabei der vielleicht stärkste empirische Befund des gesamten Dokuments: „25 von 52 Pflegediensten geben an, dass Hersteller oder IT-Dienstleistende für Wartungszwecke einen permanenten Netzwerkzugang zum Pflegedienst haben“ (DiPS-Abschlussbericht 3.8). Fast die Hälfte der befragten Dienste hat damit eine dauerhaft offene Tür ins eigene Netzwerk. Ergänzend belegt der Penetrationstest, dass auch die hinterlegten Zugangsdaten selbst regelmäßig problematisch sind — „teilweise enthielten Installationspakete statische API-Schlüssel oder Datenbankpasswörter“ (DiPS-Abschlussbericht 4.2). Die BSI-Empfehlung, Wartungszugänge „in Absprache mit dem Hersteller […] zu dokumentieren“ und „nur während Wartungsvorgängen“ zu aktivieren, verschiebt die Verantwortung erneut zur Betreiberin. Im realen Pflegealltag wird jedoch kein ambulanter Dienst gegenüber einem Hersteller eine Wartungszugang-Vereinbarung neu verhandeln, wenn das System sonst nicht läuft. Diese strukturelle Asymmetrie ist nicht auflösbar, ohne die Hersteller in die Verantwortungskette aufzunehmen. Der Deutsche Pflegerat hat genau dies in seinem Expert:innenpapier „Cybersicherheit in der pflegerischen Versorgung“ (Juni 2025) gefordert: verbindliche IT-Sicherheitsstandards für Hersteller und eine Zertifizierung der Produkte nach klar definierten Kriterien.
In der hier vorgestellten Implementierung wurde der globale, im Quellcode hinterlegte API-Schlüssel im Selbst-Audit als kritischer Befund identifiziert und mit der M1-Sicherheits-Härtung im Mai 2026 abgeschafft (siehe Anhang B.5a, M1.3). Jede Installation hält ihren eigenen, beim ersten Start generierten Schlüssel; eine ENV-Variable ist ausschließlich als Test-Override vorgesehen. Ein dauerhafter Wartungszugang für den Hersteller ist technisch nicht vorgesehen — die Open-Source-Auslieferung unter AGPLv3 macht eine entsprechende Vereinbarung zudem optional, nicht zur technischen Voraussetzung des Betriebs.

5.4 Zu BSI-Kapitel 3.4 (Schutz von mobilen Geräten)

Die Empfehlungen in BSI 3.4 — Geräteverschlüsselung, sichere Entsperrcodes und zeitnahe Updates (3.4.1) sowie eine größenabhängige Wahl zwischen Mobile Device Management und organisatorischen Regeln (3.4.2) — sind in sich konsistent. Die Beobachtung, dass „eine MDM-Software aus ökonomischen Gründen nicht immer sinnvoll [ist]“ für kleinere Dienste, trifft die Realität: jährliche MDM-Lizenzkosten pro Gerät übersteigen in kleinen Pflegediensten regelmäßig den Wert des Geräts selbst.
Die Empfehlung betrachtet das mobile Gerät jedoch als isolierten Sicherheitsraum (Verschlüsselung, Code, Update). In der ambulanten Pflegerealität entstehen die meisten Datenpannen jedoch nicht durch ein Versagen dieser technischen Maßnahmen, sondern in den organisatorischen Schnittstellen davor: geteilte Anmeldungen, wenn eine Pflegekraft der Kollegin schnell aushilft, weil die App gerade nicht reagiert; Schichtwechsel ohne korrekte Abmeldung. Beides lässt sich technisch nicht durch Geräteverschlüsselung adressieren. Ein dritter Fall — der Verlust des mobilen Geräts bei Patiententransporten oder Fahrzeugaufbrüchen — zeigt zudem, dass die in BSI 3.4.1 geforderte Verschlüsselung nur die ruhenden Daten schützt; das eigentliche Problem im Verlustfall ist das Fehlen einer Remote-Wipe-Möglichkeit ohne MDM, das den kleinen ambulanten Diensten aus den genannten

ökonomischen Gründen nicht zur Verfügung steht.
Die hier vorgestellte Implementierung stellt aktuell keine eigene mobile App, sondern ein webbasiertes Arzt-Portal bereit, das über jeden mobilen Browser nutzbar ist. Dedizierte mobile Programme als integraler Bestandteil des Ökosystems sind für die Phase nach der M1-Sicherheits-Härtung vorgesehen (siehe Roadmap-Verweis in Anhang B); sie werden vom Start an die im DiPS-Bericht erkannten Befundmuster (Hardcoded-Credentials, fehlende Server-Authentifizierung) als Designvorgaben adressieren.

5.5 Zu BSI-Kapitel 3.5 (Umsetzung von Herstellerempfehlungen)

Härtungsempfehlungen der Hersteller werden in der pflegerischen Praxis selten angefasst, weil sie schlicht nicht bekannt sind. Die in BSI 3.5 formulierte Empfehlung, sich aktiv beim Hersteller nach einer Dokumentation der Sicherheitseinstellungen zu erkundigen und diese umzusetzen, adressiert damit ein reales Defizit.
Die Empfehlung setzt jedoch drei Voraussetzungen, die das DiPS-Dokument an dieser Stelle nicht weiter prüft: erstens, dass der Hersteller eine solche Dokumentation überhaupt liefert; zweitens, dass diese für eine Betreiberin ohne IT-Hintergrund abarbeitbar ist; drittens, dass die im Dokument empfohlenen Einstellungen im Auslieferungszustand der Software überhaupt änderbar sind. Erneut entlässt die Empfehlung den Hersteller aus der Verantwortung — die betreibende Pflegeeinrichtung soll umsetzen, was der Hersteller dokumentiert hat. Hier wiederholt sich die in 5.1 und 5.3 benannte Hersteller-Betreiber-Asymmetrie.
Bei Open-Source-Software unter AGPLv3 verschiebt sich das Verhältnis: Sicherheitsrelevante Einstellungen sind im Quellcode, in den modulweisen CHANGELOG-Dateien und in der Release-Spur dokumentiert. Die in Anhang B beschriebene Audit-Spur der hier vorgestellten Implementierung ist vollständig öffentlich einsehbar. Eine Betreiberin oder ein beauftragter IT-Dienstleister kann jede Einstellung nicht nur nachlesen, sondern auch ihre Wirkung gegen den Code prüfen. Das ist ein Niveau an Nachvollziehbarkeit, das proprietäre Härtungsrichtlinien strukturell nicht erreichen.

5.6 Zu BSI-Kapitel 4.1 (Risikomanagement)

Die Erkenntnis in BSI 4.1, dass ein vollständiges Information Security Management System „für kleine Einrichtungen mit kleiner Infrastruktur und damit kleiner Angriffsfläche nicht immer sinnvoll“ ist, ist realistisch und sehr begrüßenswert. Sie vermeidet die in der Branche verbreitete Falle, kleinen Diensten eine Compliance-Last aufzuerlegen, die ihre Personalressourcen übersteigt. Auch die alternative Mindestanforderung — „schriftliche Erfassung“ der Risiken plus „vollständige Dokumentation des Pflegedokumentationssystems“ — ist als Minimal-Position sachlich vertretbar.
In der ambulanten Kleinstdienst-Realität überfordert allerdings auch diese reduzierte Anforderung. Ein Penetrationstest kostet typischerweise einen fünfstelligen Betrag, ist für einen einzelnen Pflegedienst nicht refinanzierbar und wäre als systemspezifischer Test ohnehin nicht ein einzelnes Mal, sondern pro Software-Release sinnvoll. Eine vollständige System-Dokumentation des Pflegedokumentationssystems kann ein Kleinstdienst nicht selbst erstellen — sie liegt beim Hersteller und ist Betreibenden in der Regel nicht zugänglich. Der Personalstand erlaubt selten die geforderte schriftliche Risikoanalyse jenseits der akut nötigen Pflegedokumentation.
Aus dieser Differenzierung ergibt sich eine konkrete Empfehlung an das BSI: Eine Förderpfad-Initiative gemeinsam mit den Pflegekassen zu entwickeln, die (a) Pentest-Förderung für die jeweils eingesetzten Pflegedokumentationssysteme

bündelt — Förderung über die Hersteller, nicht über den einzelnen Dienst, damit die Ergebnisse der getesteten Produktversion allen Nutzerinnen zugutekommen — (b) Risikoerfassungs-Templates in pflegegerechter Sprache bereitstellt und (c) ein „ISMS-Light“-Modell mit reduziertem Pflichtenumfang für ambulante Kleinstdienste entwickelt. Ohne einen solchen Förderpfad bleibt BSI 4.1 für die genannte Mehrheit der ambulanten Pflegedienste ein Papier-Ziel.
Das im Anhang B beschriebene Selbst-Audit zeigt, dass strukturierte, dokumentierte Risikoerfassung auch für ein eigenständig entwickeltes Pflegedokumentationssystem leistbar ist — allerdings erst durch externe Methodenunterstützung in Form des BSI-DiPS-Befundkatalogs als Maßstab. Genau dieses Muster — extern bereitgestellter Maßstab und selbst durchgeführte Erfassung — könnte Grundlage des oben skizzierten Förderpfads sein.

5.7 Zu BSI-Kapitel 4.2 (Physische Sicherheit)

Der in BSI 4.2 gezogene Vergleich — „der Umgang sollte wie bei Papierakten mit Daten Pflegebedürftiger erfolgen“ — ist als Faustregel gut gewählt. Pflegekräfte verstehen die Analogie sofort, weil sie den Umgang mit Pflegedokumentations-Ordnern aus der vor-digitalen Zeit oder aus weiterhin papierbasierten Teilstrecken kennen. Auch der Hinweis auf die Restangriffsvektoren bei verschlüsselten Systemen (USB-Schnittstellen, Ethernet) ist sachlich richtig: Festplattenverschlüsselung schützt das ruhende System, nicht das eingeschaltete.
Die Aufforderung, das mobile Gerät „im Sichtfeld zu lassen oder einzuschließen“, trifft jedoch eine pflegerische Wirklichkeit, die sie nicht erreichen kann. Pflegekräfte haben während einer Behandlung in der Regel beide Hände am Patienten — bei Lagerungswechsel, Wundversorgung, Verbandwechsel, Mobilisation oder Injektion. Das mobile Gerät liegt in dieser Zeit notwendigerweise außerhalb des Sichtfelds: auf dem Pflegebett, auf einem Tisch oder Stuhl im Nebenraum, in der Pflegetasche oder im Auto. „Einschließen“ ist im Hausbesuchskontext praktisch nicht möglich, weil keine pflegediensteigenen Schließfächer in der Wohnung der Pflegebedürftigen existieren. Die Empfehlung bleibt im stationären Kontext — etwa an einem KIS-Arbeitsplatz mit fest installiertem PC — realistisch; in der ambulanten Pflegepraxis ist sie strukturell nicht umsetzbar.
Eine lokal arbeitende, geräte-individuelle Implementierung kann die Folgen eines Geräteverlusts auf das jeweilige Endgerät begrenzen. In der hier vorgestellten Implementierung ist der API-Schlüssel pro Installation generiert (siehe Anhang B.5a, M1.3); ein verlorenes oder entwendetes Endgerät erlaubt keinen Online-Zugang zu zentralen Patientendaten. Das adressiert nicht die in BSI 4.2 formulierte Empfehlung selbst, aber den dort beschriebenen Folgeschaden.

5.8 Zu BSI-Kapitel 4.3 (Offboarding von Mitarbeitenden)

Die Empfehlung in BSI 4.3 ist sachlich vollständig, der Hinweis auf Cloud-Zugänge die genau richtige Pointierung. Cloud-Zugänge sind im Offboarding der häufigste Restzugang, weil sie weder am Schlüsselbund hängen noch im Arbeitslaptop liegen, der zurückgegeben werden muss — sie sind unsichtbar vorhanden, bis sie aktiv deaktiviert werden.
Ambulante Pflegedienste haben besonders hohe Mitarbeiter-Fluktuation: befristete Verträge, Springer-Kräfte, Aushilfen für Krankheitsvertretungen. Offboarding-Vorgänge sind dort kein Sonderfall, sondern Routine. Ein klar definierter, nachprüfbarer Ablauf — wie das BSI ihn fordert — ist daher keine Compliance-Idealvorstellung, sondern Betriebsnotwendigkeit. Ein dritter Punkt verschärft diese Routine: Software-Auswahlentscheidungen, die zusätzliche Cloud-Zugänge in den Workflow einführen — etwa SaaS-Tools für Dienstplanung,

Messaging oder Abrechnungs-Portale — vervielfachen den Offboarding-Aufwand pro Mitarbeiterin entsprechend. Auch hier zeigt sich die in 5.9 ausführlich behandelte Linie: Architekturentscheidungen wirken bis ins organisatorische Tagesgeschäft.
In einer Implementierung ohne Cloud-Komponente reduziert sich das Offboarding auf eine einzige Aktion: die Deaktivierung des Nutzerkontos in der zentralen Mitarbeiter-Datenbank des Pflegedokumentationssystems. Die hier vorgestellte Implementierung dokumentiert diese Aktion im Änderungsprotokoll mit Benutzerkontext (Audit-Trail, im DiPS-Audit als positiver Befund OF-06 bestätigt). Die fehlende Cloud-Komponente macht den Offboarding-Vorgang nicht nur einfacher, sondern auch nachprüfbar abgeschlossen.

5.9 Zu BSI-Kapitel 4.4 (Berücksichtigung von Softwareeigenschaften)

BSI 4.4 adressiert ein reales Problem — kleinere Pflegedienste haben tatsächlich Konfigurations-Risiken bei lokaler Installation, weil die nötige IT-Kompetenz im Personalstand selten verfügbar ist. Die Sorge ist legitim und sollte in einer Stellungnahme nicht bestritten werden. Diese Sektion widmet sich nicht der Beobachtung selbst, sondern der daraus abgeleiteten Empfehlungs-Tendenz, die das BSI in folgendem Zitat formuliert: „Anwendungen, die ausschließlich in der Cloud vom Hersteller betrieben werden, verursachen dagegen weniger Aufwand aufseiten des Pflegedienstes. Zudem ist das Risiko einer fehlerhaften Konfiguration geringer, da sie von entsprechend qualifiziertem Personal durchgeführt wird.“ (BSI 4.4)
Diese Empfehlungs-Tendenz nimmt die Verfügbarkeits-Asymmetrie nicht in den Empfehlungsbereich auf. Bei einem Cyberangriff auf einen Cloud-Anbieter ist nicht ein Pflegedienst betroffen, sondern alle Kunden des Anbieters gleichzeitig — ein Multi-Tenant-Effekt, der für zentralisierte IT-Infrastrukturen generell gilt, auch außerhalb der Cloud. Der DiPS-Abschlussbericht verweist im Literaturverzeichnis auf zwei einschlägige Vorfälle 2024 — AWO Münsterland-Recklinghausen und Johannesstift Diakonie — beide mit Betriebsstörungen über viele Standorte hinweg (siehe 5.11 für die ausführlichere Darstellung). Verfügbarkeits-Risiken entstehen damit nicht primär durch Konfigurations-Sorgfalt, sondern durch zentralisierte Angriffsoberflächen — eine Logik, die das DiPS-Dokument im Empfehlungsbereich nicht weiter ausführt.
Patientendaten gehören nach Art. 9 DSGVO zu den besonderen Kategorien personenbezogener Daten mit erhöhter Schutzbedürftigkeit. Eine Übertragung an Cloud-Anbieter verlagert diese Schutzverantwortung in eine Vertragsstrecke (Auftragsverarbeitung nach Art. 28 DSGVO, ggf. mit Drittstaat-Übertragung nach Art. 44 ff.), die der einzelne Pflegedienst nicht selbst kontrollieren kann. Die rechtliche Schutzanforderung verschwindet nicht — sie verlagert sich auf eine Strecke, in der die Aufsicht des einzelnen Pflegedienstes nur noch indirekt wirkt.
Cloud-Lösungen schaffen darüber hinaus strukturelle Wechselkosten. Patientendaten liegen in proprietären Formaten beim Anbieter; eine Migration zu einem anderen Produkt erfordert Export-Schnittstellen, die häufig fehlen oder nur in eingeschränkter Form vorhanden sind. Diese Wechselkosten sind im DiPS-Dokument nicht in den Empfehlungsbereich aufgenommen, obwohl sie für eine langfristige Software-Auswahlentscheidung — wie das BSI sie selbst in 4.4 thematisiert — von erheblicher Bedeutung sind.
Der DiPS-Abschlussbericht dokumentiert in den Penetrationstests zudem Schwachstellen, die unabhängig vom Betriebsmodell auftreten: hardcodierte Zugangsdaten in Installationspaketen (DiPS-Abschlussbericht 4.2), fehlende Server-Authentifizierung in TLS-Verbindungen (4.1) und gemeinsame Datenbankkonten als Folge einer Zwei-Schicht-Architektur (4.3). Diese Befunde betreffen den Hersteller-Code, nicht den Betriebsort. Cloud-Betrieb schützt nicht

vor Hersteller-Code-Fehlern; er verlagert sie nur an einen anderen Server.
Die Alternative zur Cloud-Bevorzugung ist nicht der unbegleitete On-Premise-Betrieb mit offenen Konfigurations-Risiken, sondern eine On-Premise-Architektur, die durch BSI-Härtungsrichtlinien begleitet und durch den in 5.6 vorgeschlagenen Förderpfad ressourciell unterstützt wird. Das Konfigurations-Risiko, das BSI 4.4 berechtigt benennt, lässt sich durch sichere Defaults im Auslieferungszustand reduzieren — was eine Hersteller-Pflicht ist, nicht eine Cloud-Frage.
Die hier vorgestellte Implementierung dokumentiert, dass eine lokale Architektur ohne Cloud-Zwang mit überschaubarem Konfigurationsaufwand möglich ist: Auslieferung als Komplettsystem-ZIP mit installations-individuellen Schlüsseln und sicheren Defaults seit v0.9.0 (siehe Anhang B). Die Konfigurations-Sorgfaltsfrage wird damit nicht umgangen, sondern an der richtigen Stelle adressiert — beim Hersteller, nicht durch Verlagerung in die Cloud.

5.10 Zu BSI-Kapitel 4.5 (IT-Support und IT-Dienstleistende)

Die Beobachtung in BSI 4.5, dass externe IT-Unterstützung positiv auf die IT-Sicherheit wirken kann, ist sachlich richtig. Besonders die Empfehlung zur proaktiven Vereinbarung von Incident-Response-Verträgen — „Im Krisenfall, beispielsweise bei einem Cyberangriff, sollten sie direkt darauf zugreifen können“ (BSI 4.5) — trifft eine reale Lücke: Krisenfall ist die schlechteste Zeit für Vertragsverhandlungen.
Die Empfehlung sagt jedoch, dass Pflegedienste sich „um Unterstützung […] bemühen“ sollten. Sie sagt nicht, wer diese Unterstützung anbietet, in welchem Markt sie verfügbar ist und wer sie bezahlt. Die wirtschaftliche Realität kleiner ambulanter Pflegedienste lässt regelmäßige Incident-Response-Verträge oft nicht zu. Auch hier greift der in 5.6 vorgeschlagene Förderpfad: Incident-Response-Bereitschaft ist eine plausible Förderkategorie, weil sie strukturell überindividuell wirkt — ein vorbereiteter Dienstleister kann mehreren Pflegediensten gleichzeitig zur Verfügung stehen.
Eine Open-Source-Auslieferung der Pflegedokumentations-Software erweitert den Markt qualifizierter Wartungs-Dienstleister: Jeder IT-Dienstleister kann das System administrieren — die Auswahl ist nicht auf zertifizierte Partner des Herstellers beschränkt. Das senkt die Markteintrittshürde und kann die Verfügbarkeit von Unterstützung im ländlichen Raum verbessern, wo viele ambulante Pflegedienste arbeiten. Die hier vorgestellte Implementierung ist als Komplettsystem-ZIP unter AGPLv3 verfügbar; die in Anhang B beschriebene Audit-Spur und die modulweisen CHANGELOG-Dateien geben einem beauftragten IT-Dienstleister eine vollständige Wartungs-Grundlage.

5.11 Bemerkenswerte Lücken in den DiPS-Handlungsempfehlungen

Drei Themen, die in den DiPS-Handlungsempfehlungen ein eigenes Kapitel verdienen würden, sind im aktuellen Dokumentstand nicht in den Empfehlungsbereich aufgenommen. Diese Sektion benennt die drei Lücken und schlägt jeweils eine Aufnahme vor.
Erste Lücke — Backup. Das DiPS-Dokument enthält kein eigenes Kapitel zu Backup-Strategie, und die Checkliste in Anhang A führt keinen Backup-Punkt auf. Backups sind aber zentral für Cyberangriffs-Resilienz: insbesondere Ransomware-Angriffe lassen sich nur über funktionierende, getrennt aufbewahrte Backups beheben. Vorschlag: Aufnahme eines eigenen Kapitels „Backup-Strategie“ mit (a) der 3-2-1-Regel als Mindeststandard — drei Kopien, zwei verschiedene Medien, eine außer Haus — (b) der Anforderung an Offline- bzw. Air-Gap-Backups, die sich nicht über das gleiche Netzwerk angreifen lassen, und (c) regelmäßigen Recovery-Tests, weil ein nie getestetes Backup faktisch kein Backup ist. In der hier vorgestellten Implementierung wurde mit Task #20

der Backup-Scope um die drei Sicherheits-Dotfiles erweitert (siehe Anhang B.5a) — ein konkretes Beispiel für die Operationalisierung einer solchen Backup-Strategie bei einem Pflegedokumentationssystem.
Zweite Lücke — Notfallkonzept und analoger Fallback. Das DiPS-Dokument enthält kein Kapitel zu Notbetriebsfähigkeit oder analogem Stift-und-Papier-Fallback bei IT-Ausfall. In der Pflege ist dieser Aspekt essenziell, weil eine Versorgungspflicht nach SGB XI besteht — auch bei IT-Ausfall müssen Patientinnen und Patienten weiterversorgt werden. Konkrete Belege sind im Literaturverzeichnis des DiPS-Abschlussberichts selbst zitiert: Der Cyberangriff auf die AWO Münsterland-Recklinghausen im April 2024 legte die Mailsysteme von rund 300 Einrichtungen einschließlich ambulanter Pflegedienste lahm. Der Cyberangriff auf die Johannesstift Diakonie im Oktober 2024 verschlüsselte den Großteil der IT-Systeme über 80 Standorte in mehreren Bundesländern (Schwerpunkt Berlin/Brandenburg), mit teilweiser Umstellung der Behandlungs-Dokumentation auf Papier. Das BSI nennt diese Vorfälle im Bericht, übersetzt sie im Empfehlungsdokument aber nicht in eine Notbetriebs-Empfehlung. Vorschlag: Aufnahme eines Kapitels „Notbetriebsfähigkeit“ mit (a) dokumentiertem Papier-Fallback pro Pflegeprozess, (b) Übungspflicht analog zum Brandschutz und (c) klar definierten Eskalationspfaden während eines Ausfalls.
Dritte Lücke — Schulung der Anwender. Schulung ist im DiPS-Dokument nur in 4.5 als Bei-Punkt erwähnt: „Schulungen von Herstellern können den Mitarbeitenden dabei helfen, das Pflegedokumentationssystem korrekt zu bedienen und damit Sicherheitsrisiken durch fehlerhafte Bedienung zu minimieren“ (BSI 4.5). Es gibt kein eigenes Schulungs-Kapitel und keinen Schulungs-Punkt in der Checkliste. Diese Lücke ist besonders auffällig, weil die im Penetrationstest dokumentierten Befunde nicht alle Hersteller-Code-Probleme sind — viele entstehen aus Wissenslücken bei Konfiguration und Betrieb. Pflegeschulen als bestehende Träger der Awareness-Bildung sind im DiPS-Dokument nicht adressiert. Vorschlag: Aufnahme eines Kapitels „Schulung und Awareness“ mit (a) einem verbindlichen Schulungs-Curriculum für Pflegekräfte, (b) Einbindung der Pflegeschulen als bestehende Bildungsinfrastruktur und (c) einer Hersteller-Pflicht zur Bereitstellung anwenderorientierter Schulungsmaterialien.
Pflegeschulen sind als geschützte Lehrumgebung ohne Echtdaten eine naheliegende erste Erprobungsumgebung für eine solche Schulungs-Strecke — und damit eine strukturelle Antwort auf das Fehlen eines Schulungs-Kapitels im DiPS-Dokument.

5.12 Zur Checkliste in BSI-Anhang A

Die Checkliste in BSI-Anhang A ist als Format hilfreich — sie macht die Empfehlungen für eine ambulante Pflegeeinrichtung abarbeitbar und gibt einen klaren Selbst-Überprüfungs-Rahmen. Die Strukturierung entlang der BSI-Kapitel ist konsistent.
Vorschlag zur Ergänzung der Checkliste um die drei in 5.11 benannten Lücken: ein Abschnitt „Backup“ mit den Items „3-2-1-Backup vorhanden“, „Offline-Backup vorhanden“, „Recovery-Test in den letzten 12 Monaten dokumentiert“; ein Abschnitt „Notbetriebsfähigkeit“ mit den Items „dokumentierter Papier-Fallback vorhanden“, „letzte Notbetriebs-Übung in den letzten 12 Monaten dokumentiert“, „Eskalationspfad während eines Ausfalls bekannt“; ein Abschnitt „Schulung“ mit den Items „Schulungsplan vorhanden“, „letzte Awareness-Schulung in den letzten 12 Monaten dokumentiert“, „Hersteller-Schulungsmaterial verfügbar“.
Zur Form der Checkliste eine Anmerkung: Die Ja/Nein-Spalte erfasst Zustände binär. Im Pflegealltag sind viele Maßnahmen jedoch nur teilweise umgesetzt —

etwa ein MDM für nur die Hälfte der Geräte oder eine Geräteverschlüsselung nur auf Tablets, nicht auf Laptops. Eine ergänzende Vier-Wege-Bewertungs-Skala („ja“ / „teilweise“ / „nein“ / „nicht zutreffend“) als einzelne Auswahl-Spalte könnte Falschmeldungen in die Ja-Spalte vermeiden und die Aussagekraft der Selbst-Überprüfung erhöhen.
Die Audit-Spur in audit/dips_2026/ enthält ein verwandtes Format: 55 Befunde mit ID, Modul, Fundstelle, Tragweite und Lösungsvorschlag (siehe Anhang B.5). Eine solche tabellarischstrukturierte Erfassung wäre auch für Checklisten-Ergänzungen in BSI-Anhang A ein anschlussfähiges Format.

6. Vorschlag: ergänzende Empfehlungen

Die folgenden Empfehlungen fassen die in den vorigen Kapiteln entwickelten Vorschläge zusammen und ergänzen sie um zwei strukturelle Forderungen, die in dieser Stellungnahme zuvor nur am Rand angesprochen wurden.
1. Open-Source-Architekturen mit lokaler Datenhaltung als gleichberechtigte Variante in die DiPS-Handlungsempfehlungen aufnehmen. Ausführliche Begründung in Kapitel 4, insbesondere 4.4; Bezugsrahmen FSFE „Public Money — Public Code“ und Sovereign Tech Agency in Anhang C.
2. Größenklassen-differenzierte Empfehlungspakete für ambulante Pflegedienste entwickeln — als pragmatische Faustregel etwa in den Klassen bis fünf Mitarbeitende, sechs bis 25 sowie über 25 Mitarbeitende. Ausführliche Begründung in 3.2; für die mittleren und kleineren Klassen ist der in 5.6 vorgeschlagene Förderpfad die ressourcielle Verstärkungs-Strecke.
3. Ein hersteller-adressiertes Schwesterdokument für Pflegedokumentationssysteme entwickeln, analog zur SiPra-Konstruktion für Praxisverwaltungssysteme. Ausführliche Begründung in 3.1; anschlussfähig an die Forderungen des Deutschen Pflegerats vom Juni 2025 (siehe 5.3 und Anhang C).
4. KRITIS-Schwellen für ambulante und stationäre Pflege im Lichte der dokumentierten Cyber-Vorfälle überprüfen. Die Pflege ist faktisch kritische Infrastruktur — die Versorgungspflicht nach SGB XI gilt auch bei IT-Ausfall, und die in Kapitel 5.9 und 5.11 referenzierten Vorfälle bei der AWO Münsterland-Recklinghausen (April 2024) und der Johannesstift Diakonie (Oktober 2024) haben die Sektor-Wirkung von Cyberangriffen auf Pflegestrukturen belegt. Die EU-Richtlinie 2022/2555 (NIS2) und das deutsche Umsetzungsgesetz NIS2UmsuCG (in Kraft seit Dezember 2025) nehmen häusliche Pflegedienste und Pflegeheime jedoch explizit aus dem Anwendungsbereich aus. Diese Ausnahme ist im Lichte der dokumentierten Vorfälle zu überprüfen — entweder durch Aufnahme der Pflege in den NIS2-Anwendungsbereich, durch Absenkung der KRITIS-Schwellen für Pflege-spezifische Einrichtungen oder durch eine eigene KRITIS-Klassifikation für die Pflege im Rahmen des KRITIS-Dachgesetzes.
5. Berücksichtigung der ePA- und TI-Anbindung von Pflegedokumentationssystemen als Sicherheits-Anforderungs-Feld in den Handlungsempfehlungen. Pflegeeinrichtungen sind seit 1. Juli 2025 zur Anbindung an die Telematikinfrastruktur verpflichtet; die ePA für alle befindet sich seit Januar 2025 im Opt-out-Modell und seit Oktober 2025 im verpflichtenden Regelbetrieb in allen medizinischen Einrichtungen. Die spezifischen Sicherheits-Anforderungen an Pflegedokumentationssysteme, die diese Anbindung tragen — etwa hinsichtlich elektronischer Medikationsliste, Pflege-Kommentaren in der ePA oder Abrechnung über KIM —, sind in den DiPS-Handlungsempfehlungen bislang nicht erfasst. Diese Anschluss-Frage gehört in den Empfehlungsbereich aufgenommen, weil die Integration im Pflegealltag bereits vollzogen wird (Quellen-Hinweise zu TI/ePA in Anhang C).

6. Aufnahme der in Kapitel 5.11 dieser Stellungnahme vorgeschlagenen drei strukturellen Lücken in die DiPS-Handlungsempfehlungen — Backup-Strategie, Notbetriebsfähigkeit mit analogem Fallback, sowie Schulung und Awareness der Anwender. Begründung, konkrete Vorschläge zur inhaltlichen Ausgestaltung (jeweils mit Unterpunkten a/b/c) sowie Anschluss an dokumentierte Vorfälle und an die bestehende Bildungs-Infrastruktur der Pflegeschulen in 5.11.

7. Zusammenfassung

Die DiPS-Handlungsempfehlungen sind in der Sache richtig und überfällig. Die Befundklassen, die der Penetrationstest dokumentiert hat, treffen reale Schwachstellen in der deutschen Pflege-IT, und die Empfehlungen adressieren sie überwiegend zutreffend. Das Verfahren — öffentliche Konsultation, Coordinated Vulnerability Disclosure mit den Herstellern, transparente Auswahl von drei marktrelevanten Systemen — entspricht einem Standard, der in der deutschen IT-Sicherheits-Aufsicht keineswegs Standard ist. Die Schwäche der Empfehlungen liegt nicht in dem, was sie sagen, sondern in dem, was sie offenlassen: Sie sind asymmetrisch zwischen Hersteller- und Betreiber-Adressaten verteilt, sodass eine ganze Befundklasse — Mängel im Hersteller-Code — durch betreiberseitige Maßnahmen strukturell nicht erreichbar ist (Kapitel 3.1).

Hinter dieser Asymmetrie wirkt eine zweite, unausgesprochene Setzung: das Marktbild proprietärer, vom Hersteller gepflegter Cloud- und Client-Server-Software wird als gegeben vorausgesetzt, ohne als Annahme markiert zu sein (Kapitel 4.1). Die Empfehlungen lesen sich von dieser stillen Voraussetzung aus folgerichtig — sie verlieren ihre Schlüssigkeit jedoch, sobald man die Voraussetzung selbst zum Gegenstand macht. Eine alternative Architektur, in der Sicherheits-Konfiguration im Quellcode dokumentiert ist statt in einer Hersteller-Anleitung, in der Patientendaten auf dem Trägersystem der Einrichtung bleiben statt in einem Cloud-Vertragsverhältnis, verlangt die meisten der vom BSI empfohlenen betreiberseitigen Strecken schlicht nicht.

Daraus folgt der Kernsatz dieser Stellungnahme: Open Source mit lokaler Datenhaltung ist im Pflegekontext nicht eine Variante, die „auch möglich“ wäre, sondern eine strukturell besser geeignete Antwort auf mehrere der vom BSI selbst benannten Schwachstellen-Cluster — von TLS-Konfigurationsmängeln über hardcodierte Zugangsdaten bis zur Hersteller-Wartungs-Asymmetrie (Kapitel 4). Diese Position ist nicht spekulativ. Sie wird im Anhang B durch eine ausgelieferte Implementierung mit Selbst-Audit gegen den DiPS-Befundkatalog belegt — eine Implementierung, die zeigt, dass die Architekturoption nicht nur denkbar, sondern bereits umsetzbar ist.

Der Verfasser steht dem BSI für eine Mitwirkung an einer überarbeiteten Fassung der Handlungsempfehlungen zur Verfügung — sei es zur fachlichen Diskussion einzelner Empfehlungstexte, sei es im Rahmen von Pilotprojekten an Pflegeschulen und Lehrbetrieben oder einer strukturierten Praxistests-Phase mit ambulanten Pflegediensten. Die hier vorgelegten Vorschläge sind als konstruktive Erweiterung gemeint, nicht als Gegenposition; ihre Aufnahme in den Empfehlungsbereich würde die Wirksamkeit der DiPS-Empfehlungen aus Sicht des Verfassers strukturell erhöhen.

Anhang

A — Kurzprofil des Verfassers

Der berufliche Weg des Verfassers beginnt im ambulanten Bereich: Die Umschulung zum Altenpfleger (Abschluss 2007) absolvierte er mit ambulantem Schwerpunkt, ausgerichtet auf die Versorgung sozial benachteiligter, häufig chronisch und mehrfach erkrankter Menschen. Aus diesem Ursprung erwuchsen zwei fachliche Vertiefungen, die ihn bis heute prägen: die Wundversorgung, für die er die Weiterbildung zum Wundassistenten nach dem ersten Curriculum der Deutschen Gesellschaft für Wundheilung absolvierte und mit der er bis heute praktisch befasst ist, und die Schmerzversorgung, über eine Weiterbildung in der Schmerzpflege bei der Akademie des Arbeiter-Samariter-Bundes, die dem damaligen algesiologischen Fachassistenten nach dem ersten Curriculum der Deutschen Gesellschaft zum Studium des Schmerzes entsprach. In beiden Feldern hat der Verfasser die fachliche Haltung aus der Entstehungsphase der jeweiligen Standards aufgenommen.
Nach einem Wechsel in den stationären Bereich erweiterte sich das Profil um das Qualitätsmanagement, um eine Stabsstellen-Tätigkeit als Assistent von Einrichtungsleitungen sowie um Erfahrung in der Funktion einer Pflegedienstleitung bei einem gemeinnützigen Träger. Die Qualifikation als Praxisanleiter (2015) ergänzt die Reihe. Insgesamt umfasst der Werdegang rund acht bis neun Jahre ambulante Tätigkeit sowie mehrere Jahre stationäre Pflege und Leitungsnähe.
Der Praxisbezug ist aktuell und mehrfach verankert: Der Verfasser ist gegenwärtig weiterhin in Teilzeit in einem stationären Pflegeheim in der Region Flensburg tätig. Als freiberuflicher Dozent für Pflegeeinrichtungen — überwiegend für ambulante Pflegedienste — steht er zugleich im laufenden Austausch mit der Leitungsebene seiner Kundeneinrichtungen und kennt deren organisatorische und dokumentarische Probleme aus erster Hand.
Aus dieser Verankerung speist sich auch die Perspektive auf die IT-Sicherheit: Der Verfasser kennt die gelebte Sicherheitsrealität im Pflegealltag — den oft unsicheren Umgang mit Passwörtern, die Überforderung kleiner Betriebe bei der Absicherung von Netz und Geräten, und die Lücke zwischen einer pflegefern entwickelten Software und dem, was die Versorgung tatsächlich braucht. Diese Lücke und ein zu dünner Markt unabhängiger IT-Dienstleister bilden den Hintergrund, vor dem der Verfasser ein vollständig quelloffenes, lokal betriebenes Pflegesoftware-Ökosystem entwickelt hat. Leitend ist dabei ein durchgängiges Motiv: eine gerechte, personenzentrierte Versorgung — für Pflegebedürftige wie für Pflegende — und die Loslösung von kommerziellen Abhängigkeiten, die sich zwischen Versorgung und Fachlichkeit drängen.

B — Technisches Kurzprofil PflegeDoku Pro

B.1 Überblick

PflegeDoku Pro ist ein Ökosystem aus sieben eigenständigen Fachprogrammen, die zusammen einen vollständigen Pflegedokumentations- und Verwaltungsstack ohne Cloud-Komponente bilden. Architekturprinzipien: lokale Datenhaltung, Loopback-Kommunikation zwischen den Modulen, AGPLv3-Lizenz für alle sieben Programme, reproduzierbarer Auslieferungsstand über annotierte Git-Tags (v0.9.0).
Versionsstand: v0.9.0, M1-gehärtetes Pre-Release, ausgeliefert 2026-05-20 als

auditfestes Komplettsystem-ZIP (1,6 MB gepackt, 500 Einträge, alle sieben Module konsistent auf 0.9.0). Versionskonsistenz wurde über fünf Bereinigungs-Passes hergestellt; die 388 Python-Dateien und 13 Bash-Skripte des Auslieferungspakets sind syntaktisch fehlerfrei (AST-Parse bzw. bash -n).
Tech-Stack:
– Sprache: Python 3.10+, rund 148.000 Python-Zeilen über die sieben Module (Stand 2026-05-20, gemessen mit wc -l ohne venv/Cache).
– GUI: PyQt6.
– Datenhaltung: SQLite je Programm; in PflegeDoku Pro und Intelligence sind sicherheitsrelevante Felder mittels Fernet (AES-128 in CBC mit HMAC-SHA256, cryptography-Bibliothek) verschlüsselt; der symmetrische Schlüssel liegt in ~/PflegeDokuDaten/.keys/encryption.key mit chmod 0600. SQLite-Container-Verschlüsselung (z. B. SQLCipher) ist nicht implementiert. Abrechnung arbeitet mandantenfähig mit JSON-Dateien.
– Interprogramm-Kommunikation: REST über Loopback — FastAPI auf Port 8080 mit X-API-Key-Header, Flask auf Port 5010 mit HTTP Basic Auth. Default-Bind seit v0.9.0 auf 127.0.0.1, LAN-Bind nur nach explizitem Konfigurationsschritt. Keine öffentlich erreichbaren Endpunkte.
– KI-Komponente (optional, ausschließlich in Intelligence): lokales LLM über ollama mit Mistral 7B; keine Cloud-LLM-Anbindung.
– Trägersystem: jedes übliche Linux-Mint- oder Ubuntu-System (64-bit).
Lizenz: AGPLv3 (alle sieben Module einheitlich).

B.2 Module im Überblick

1	PflegeDoku Pro	Pflegedoku, SIS, Bewohnerdaten, Vitalwerte, Medikation, REST-API	frei
2	PflegeDoku Pro Abrechnung	Pflegekassen-, Heimkosten-, Privatzahler-Abrechnung; ZUGFeRD 2.1, DTA/EDIFACT (SLLA)	frei
3	PflegeDoku Pro Dienstplan	ArbZG-konforme Schichtplanung, PeBeM-Konformität, eigene Abrechnungs-API (Port 5010)	frei
4	Mitarbeiter Abrechnung	Lohn-/ Gehaltsabrechnung, SEPA (ISO 20022), DATEV-Export	frei
5	PflegeDoku Pro Zeiterfassung	QR-/NFC-Stempelterminal mit HMAC-SHA256-signierten Karten	frei
6	PflegeDoku Intelligence	Morgenbriefing, fünf Analysemodule, MDK-Simulator	IIa*
7	PflegeDoku Pro Systemassistent	Installation, Health-Check, Backup, Bedrohungserkennung, UFW/Timeshift/LUKS-Vorkonfiguration	frei

* Intelligence trägt klinisch-bewertende Funktionen (MDR-Klasse-IIa-relevant) und institutionsbezogene Auswertungen (MDR-frei) in getrennten Modul-Teilen; Konformitätsbewertung der klinischen Komponente folgt separat zur MDR-freien Basisversion.

B.3 Datenkreisläufe als Architekturbeleg

Die Architektur ist so geschnitten, dass Patienten-, Mitarbeiter- und Abrechnungsdaten das Trägersystem nicht verlassen. Drei Mechanismen tragen das:
– Netzwerkschicht. Sämtliche Modul-zu-Modul-Aufrufe gehen ab v0.9.0 über 127.0.0.1 (Loopback). Bestands-Konfigurationen mit host = 0.0.0.0 werden beim ersten Start nach dem Update aktiv auf 127.0.0.1 umgeschrieben (siehe M1.1 in B.5a). Ein LAN-Bind ist nur durch explizites Setzen einer Adresse in config.ini bzw. der Umgebungsvariablen DIENSTPLAN_HOST möglich; ein öffentliches Exposing ist nicht vorgesehen und wird vom Bordmittel-Reverse-Proxy-Bereich des Systemassistenten nur mit zusätzlicher TLS-Vorlage unterstützt.
– Authentisierungsschicht. Ab v0.9.0 hat jede Installation eigene Geheimnisse — kein im Quellcode festgelegter Default. Drei Schlüsseldateien werden beim ersten Start unter ~/PflegeDokuDaten/ mit chmod 0600 angelegt: .api_key (32 Bytes urlsafe-Random für die REST-API), .jwt_secret (Arzt-Portal-JWT-Secret) und .keys/encryption.key (Fernet-Schlüssel für den EncryptedString-Layer). Die vier API-Key-Konsumenten-Module (Abrechnung, Dienstplan, Mitarbeiter Abrechnung, Systemassistent) lesen den von PflegeDoku Pro generierten Schlüssel schichtweise (ENV-Variable für Test/CI → .api_key-Datei → Modul-DB) und lehnen die Sentinel-Werte abgeschaffter Klartext-Defaults auf jeder Schicht ab.
– Verschlüsselungsschicht. Sicherheitskritische Felder sind über einen Fernet-basierten EncryptedString-Typ bzw. einen Helper-Aufruf transparent verschlüsselt: in der PflegeDoku-Pro-DB betrifft das das_api_password (Einrichtungs-Tabelle), in der Intelligence-Konfiguration email_smtp_pass. Patient-Stammdaten (vorname, nachname, geburtsdatum) sind in v0.9.0 noch unverschlüsselt — der Befund ist als DIPS-10-01 dokumentiert und für M2 priorisiert.
Backups erfasst der Systemassistent über das KONFIG_DATEIEN-Mapping; seit Task #20 (siehe B.5a) sind die drei Sicherheits-Dotfiles im Scope, der Restore-Pfad stellt chmod 0600 defensiv wieder her — auch bei Transport über Übertragungswege ohne preserve-permissions (tar/zip/cp ohne -p, E-Mail-Anhang, FAT-Filesystem).

B.4 Regulatorischer Status

Das Ökosystem ist regulatorisch in zwei Schichten geschnitten:
– MDR-frei: PflegeDoku Pro (Dokumentation, REST-API), Abrechnung, Dienstplan, Mitarbeiter Abrechnung, Zeiterfassung, Systemassistent — insgesamt sechs der sieben Module — sowie der institutionsbezogene Auswertungsteil von Intelligence. Diese Programme erbringen Dokumentations-, Verwaltungs- und Organisationsfunktionen, keine klinische Beurteilung im Sinne der MDR (EU) 2017/745.
– MDR-Klasse-IIa-relevant: der klinisch-bewertende Teil von PflegeDoku Intelligence (Morgenbriefing mit Pflegeempfehlungen, Analyse-Module, MDK-Simulator), soweit er Aussagen mit Bezug auf den einzelnen Patienten erzeugt. Die Konformitätsbewertung dieser Komponente erfolgt separat von der Auslieferung der MDR-freien Basis.
Lizenz: AGPLv3 (alle sieben Module einheitlich).
Die MDR-freie Basisversion „PflegeDoku Pro Basis“ steht unmittelbar vor der

Markteinführung. Die auditfeste Komplettsystem-Version 0.9.0 ist ausgeliefert; die finale Veröffentlichung der Basisversion ist im Juli 2026 vorgesehen.

B.5 Internes Audit

Das interne Audit gegen den BSI-DiPS-Befundkatalog wurde vom Verfasser selbst durchgeführt — Zeitraum 2026-04-25 bis 2026-05-06, read-only mit Cross-Review-Pass am 2026-05-06. Geprüft wurden alle sieben Module des Komplettsystems gegen die Schwachstellenklassen 1-12 der DiPS-Methodik.
Ergebnis: 55 dokumentierte Befunde, verteilt auf
– 8 kritisch
– 17 hoch
– 19 mittel
– 11 informativ (positive Bestätigungen)
– 4 Empfehlungen für noch nicht existierende Komponenten (mobile App, Fernzugriff).
Audit-Spur: vollständig schriftlich im Verzeichnis audit/dips_2026/, gegliedert in 00_zusammenfassung.md (10-Minuten-Lesepfad), 01_befunde.md (alle 55 Befunde), 02_risikomatrix.md (Tabelle mit Wahrscheinlichkeit, Aufwand, Priorität), 03_loesungsvorschlaege.md, 04_offene_fragen.md, 05_methodik.md. Pro Befund: ID, Modul, Fundstelle (Datei:Zeile), DiPS-Klasse, Wahrscheinlichkeit, Tragweite, Lösungsvorschlag.

B.5a Sofortmaßnahmen-Bilanz (M1, abgeschlossen 2026-05-20)

Acht Sofortmaßnahmen wurden zwischen 2026-05-13 und 2026-05-20 in sieben Modul-Codebasen umgesetzt, mit Pflicht-Smoke-Tests pro Maßnahme. Vollständige Maßnahmen-Spur in audit/dips_2026/CHANGELOG_DIPS_UMSETZUNG.md.

M1.1	Default-Bind auf 127.0.0.1 mit aktiver Migration der Bestands-config.ini	DIPS-05-06, DIPS-08-01, DIPS-08-02	928e55f (Pro) 8e99b72 (Dienstplan)
M1.2	JWT-Secret pro Installation (Hardcoded-Default entfernt)	DIPS-02-01	be75057 (Pro)
M1.3	Globaler API-Key abgeschafft — Schichten-Lesepattern in vier Konsumenten-Modulen	DIPS-02-02	9589c30 (Pro) + 4 Konsumenten-Commits
M1.4	BRIEFING_PIN_HASH-Karteileiche entfernt (PIN-Mechanik bereits 2026-03-24 durch Mitarbeiter-DB-Login mit bcrypt abgelöst)	DIPS-02-03	0cbc2a9 (Intelligence)
M1.5	Telematik-Router mit verify_api_key abgesichert	DIPS-03-04	2563cb7 (Pro)
M1.6	CORS-Wildcards durch enge Loopback-Allowlist ersetzt	DIPS-03-06	071b7d7 (Pro)
M1.7	Fernet-Verschlüsselung sensitiver DB-Spalten	DIPS-10-02, DIPS-11-04	dfc7f3a (Pro) 5be6746 (Intelligence)

M1.8	und JSON-Felder DEBUG-print() aus API-Login durch strukturiertes Logging ersetzt	DIPS-02-05	1d3fd8b (Pro)

Ergänzend, sicherheits-release-relevant:

#20	Backup-Scope um die drei Sicherheits-Dotfiles erweitert; chmod 0600 wird nach Restore defensiv wiederhergestellt (Latent-Bug-Fix mkdir(parents=True) im Restore-Pfad mit-behoben)	eigener Befund — Audit-Lücke, da die Dotfiles zum Audit-Zeitpunkt noch nicht existierten	8e702bf (Systemassistent)

Zur Befund-Schließung: Alle als „Sofort“ priorisierten kritischen Befunde sind mit M1 abgeschlossen. Vier kritische Befunde (DIPS-03-01, DIPS-04-01, DIPS-12-01, DIPS-12-02) verbleiben als Architektur-Backlog (M4) und sind ausdrücklich als Voraussetzungen vor ambulantem Rollout, LAN-Mehrgeräte-Setup und öffentlichem Arzt-Portal markiert — im stationären Einzelplatzbetrieb tragbar.

B.5b Audit-Korrekturen

Zwei Befund-Korrekturen sind im Verzeichnis audit/dips_2026/AUDIT_KORREKTUREN.md schriftlich dokumentiert:
– DIPS-02-03 (PIN-Mechanik): Der Audit-Lösungsvorschlag empfahl PIN-Dialog mit bcrypt und mindestens 6-stelliger PIN. Die Code-Verifikation am 2026-05-19 zeigte, dass die zugrundeliegende PIN-Mechanik bereits am 2026-03-24 durch Mitarbeiter-DB-Login (bcrypt + Rollenprüfung gegen LEITUNGS_ROLLEN) abgelöst worden war. Eine Reaktivierung wäre UX-Regression und Rollerückwärts. Umgesetzt wurde Punkt 1 des Lösungsvorschlags (Konstante und Folge-Referenzen entfernen).
– DIPS-02-02 (globaler API-Key): Die Audit-Fundstellenliste war unvollständig. Im eigenen Verifikations-Grep am 2026-05-20 wurde das Modul „Mitarbeiter Abrechnung“ als zusätzlicher Fundkreis und die Schlüssel-Variante pflegedoku_abrechnung_2025 als zusätzlicher Wert identifiziert; beide wurden in M1.3 mitbehoben.
Die Korrekturen sind transparent gehalten — sie belegen, dass Audit-Befunde nicht 1:1 in Maßnahmen übersetzt, sondern gegen den jeweils aktuellen Code-Stand verifiziert werden. Methodische Grundregel: Audit-Fundstellenlisten sind eine Untergrenze, nicht ein vollständiges Mapping.
Über M1 hinaus stehen im M2-Backlog drei dokumentierte Folgemaßnahmen: Konsolidierung des duplizierten API-Key-Loader-Helpers in ein gemeinsames Modul (Task #19), aktive Boot-Migration der verbleibenden Bestands-Klartext-Werte für das_api_password und email_smtp_pass (Task #18, ergänzend zur in M1.7 etablierten Lazy-Migration), sowie kid-Header-Mechanik für JWT-Schlüssel-Rotation ohne Service-Ausfall (Task #17, Erweiterung von M1.2). Vollständige Task-Spur in audit/dips_2026/TASKS_DIPS_UMSETZUNG.md.

B.6 Konsequenzen

Die Belege, dass v0.9.0 nicht ein angekündigter, sondern ein ausgelieferter Stand ist, sind dreischichtig:
– Auslieferungs-Disziplin. Die Erstellung des Komplettsystem-ZIPs ist in fünf

Bereinigungs-Passes erfolgt (Versionskonsistenz, AST-Parse aller Python-Dateien, bash -n für alle Shell-Skripte, Inventur-Abgleich, Manifest-Vollständigkeit). Ergebnis: 1,6 MB gepackt, 500 Einträge, alle sieben Modul-CHANGELOGs mit M1-Block, alle sieben Module konsistent auf 0.9.0.
– Maßnahmen-Disziplin. Die acht M1-Sofortmaßnahmen sind atomar pro Befund commitiert, mit Pflicht-Smoke-Tests, mit Audit-Spur-Korrektur dort, wo der Befund-Vorschlag vom Code-Stand abwich. Querschnittsmaßnahmen (M1.3 über fünf Module, M1.1 über zwei Module, M1.7 über zwei Module) tragen einheitliche Commit-Subject-Präfixe [DIPS-XX-XX] für nachvollziehbare Audit-Spur.
– Praxis-Übergang. Die Version 0.9.0 wurde Ende Mai 2026 einer Pflegeschule in Schleswig-Holstein auf deren Anfrage zur Erprobung zur Verfügung gestellt, mit strukturierter Installationsanleitung und einer Rückmeldevorlage für Praxisbeobachtungen. Konkrete Einrichtungs- und Personendaten werden in dieser Stellungnahme nicht genannt — dies entspricht der DSGVO-Sorgfalt, die der Verfasser in der gesamten Produktentwicklung anwendet. Die Wahl einer Pflegeschule als Erprobungsumgebung ist begründet: Sie ermöglicht den Einsatz im geschützten Lehrkontext ohne Echtdaten und adressiert gleichzeitig die in den DiPS-Empfehlungen unterbelichtete Frage der praktischen Schulung von Anwendern (siehe Kapitel 5.11 dieser Stellungnahme).

B.7 Reproduzierbarkeit und Detaildokumente

Reproduzierbarkeits-Anker. Die sieben Modul-Repos sind mit annotierten Git-Tags v0.9.0 versehen. HEAD-Commit-Hashes pro Modul (volle SHA-1 für BSI-Nachprüfbarkeit):
PflegeDoku Pro 9589c3082aa6b8600e37b9d7fd026d3f05c43d41
PflegeDoku Pro Abrechnung 8885a0104fa04b1a978a07edde0ce0422b70824c
PflegeDoku Pro Dienstplan 47dba65e366df7341d8ba6024b5a211797f7ab06
Mitarbeiter Abrechnung 5a8e3b2990961cfba3e6dbc1890e6436b5ff1940
PflegeDoku Pro Systemassistent 8e702bf240f9ff26d9ebd2059587dcf7fc28b7ec
PflegeDoku Intelligence 5be6746b21c2026d38b465bd964860bb658521ef
PflegeDoku Pro Zeiterfassung 9f41e31de1613060617b78e62dd004ca40452648
Auf Anfrage verfügbar (an die im Briefkopf genannte Adresse des Verfassers): das auditfeste Komplettsystem-ZIP der Version 0.9.0, der vollständige Inhalt des Verzeichnisses audit/dips_2026/ (Audit-Bericht in fünf Teildokumenten, Maßnahmen-Spur CHANGELOG_DIPS_UMSETZUNG.md, Audit-Korrekturen AUDIT_KORREKTUREN.md, Task-Spur TASKS_DIPS_UMSETZUNG.md, Release-Spur RELEASE_v0.9.0.md, Pflicht-Smoke-Test-Spur SMOKE_TESTS.md, Restore-Kompatibilitäts-Spur RESTORE_KOMPATIBILITAET.md) sowie die einzelnen Modul-CHANGELOGs.
Die Auslieferung erfolgt nicht öffentlich, sondern auf konkrete Anfrage einer beteiligten Stelle, mit dokumentiertem Empfänger-Vermerk — dies entspricht der bisherigen Audit-Praxis des Verfassers und respektiert, dass die Maßnahmen-Spur betriebs-interne Belege (Test-Konten-Kürzel, Test-Home-Pfade) enthält, die in einer öffentlichen Veröffentlichung gekürzt würden.

C — Quellen und Verweise

BSI-Dokumente

- BSI: Abschlussbericht zum Projekt „Sicherheit von digitalen Pflegedokumentationssystemen“ (DiPS), Version 1.0, 13.02.2026. bsi.bund.de
- BSI: Handlungsempfehlungen zur Verbesserung der IT-Sicherheit in ambulanten Pflegediensten (DiPS), Konsultationsfassung Version 0.9, 13.02.2026, Frist 17.06.2026. bsi.bund.de

- BSI: Abschlussbericht zum Projekt „Sicherheit von Praxisverwaltungssystemen“ (SiPra), Version 1.0, 12.02.2026. bsi.bund.de
- BSI: SiKIS — Abschlussbericht und Handlungsempfehlungen zur Sicherheit von Krankenhausinformationssystemen, 2025. bsi.bund.de
- BSI: Technische Richtlinie TR-02102-2 „Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)“, aktuelle Fassung. bsi.bund.de

Gesetzliche und regulatorische Quellen

- Verordnung (EU) 2017/745 über Medizinprodukte (MDR), in der jeweils geltenden Fassung.
- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO), insbesondere Art. 9 (besondere Kategorien personenbezogener Daten), Art. 28 (Auftragsverarbeitung) und Art. 44 ff. (Drittstaat-Übertragung).
- Sozialgesetzbuch Elftes Buch (SGB XI), insbesondere § 113 (Maßstäbe und Grundsätze für die Qualität, die Qualitätssicherung und die Qualitätsdarstellung).
- Richtlinie (EU) 2022/2555 zur Netz- und Informationssicherheit (NIS2), umgesetzt in Deutschland durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), einschließlich der KRITIS-Verordnung.

Positionspapiere und Studien

- Deutscher Pflegerat: Expert:innenpapier „Cybersicherheit in der pflegerischen Versorgung“, herausgegeben von der DPR-Expert:innen-Kommission „Digitalisierung in der Pflege“, Juni 2025. deutscher-pflegerat.de
- Free Software Foundation Europe (FSFE): „Public Money — Public Code“. publiccode.eu
- Sovereign Tech Agency (vormals Sovereign Tech Fund), Förderprogramm des Bundesministeriums für Digitales und Staatsmodernisierung. sovereign.tech

Belege zu Cyber-Vorfällen in der Pflege- und Gesundheitslandschaft (zitiert in 5.9 und 5.11)

- Cyberangriff auf die AWO Münsterland-Recklinghausen, April 2024: Lähmung der Mailsysteme von rund 300 Einrichtungen einschließlich ambulanter Pflegedienste. Belegt in der überregionalen Berichterstattung und im DiPS-Abschlussbericht zitiert.
- Cyberangriff auf die Johannesstift Diakonie, 13. Oktober 2024: Verschlüsselung des Großteils der IT-Systeme über 80 Standorte in mehreren Bundesländern (Schwerpunkt Berlin/Brandenburg), teilweise Umstellung der Behandlungs-Dokumentation auf Papier. Belegt durch Pressemitteilungen der Johannesstift Diakonie und im DiPS-Abschlussbericht zitiert.

Vorträge

- Chaos Computer Club: einschlägige Vorträge zur Telematikinfrastruktur und elektronischen Patientenakte (ePA), insbesondere auf den Jahreskongressen 35C3, 36C3 und 38C3. media.ccc.de

Eigene Vorarbeiten (auf Anfrage verfügbar)

- Internes Audit des PflegeDoku-Pro-Ökosystems gegen den BSI-DiPS-Befundkatalog, 2026-04-25 bis 2026-05-06, mit Cross-Review-Pass am

2026-05-06. 55 dokumentierte Befunde, vollständige schriftliche Audit-Spur im Verzeichnis audit/dips_2026/ (Bericht in fünf Teildokumenten, Maßnahmen-Spur, Audit-Korrekturen, Task-Spur, Release-Spur, Smoke-Test-Spur, Restore-Kompatibilitäts-Spur). Siehe Anhang B.7.