Contents

Chapter 1

HIPAA Compliance Handbuch

Dokument-Metadaten

- **Erstellt am:** 2026-02-10
- **Autor:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.5
- **Typ:** HIPAA-Handbuch

---

ewpage

Chapter 2

Geltungsbereich und Anwendbarkeit

Dokument-ID: HIPAA-0010
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

2.1 1. Zweck

Dieses Dokument definiert den Geltungsbereich der HIPAA-Compliance für AdminSend GmbH und legt die Anwendbarkeit der Anforderungen der HIPAA Security Rule, Privacy Rule und Breach Notification Rule fest.

2.1.1 1.1 Zielsetzungen

- **Geltungsbereichsdefinition:** Klare Identifizierung HIPAA-regulierter Aktivitäten und Systeme
- **Compliance-Rahmen:** Grundlage für das HIPAA-Compliance-Programm schaffen
- **Rollenklärung:** Rolle der Organisation als Covered Entity oder Business Associate definieren
- **PHI-Identifizierung:** Alle geschützten Gesundheitsinformationen im Geltungsbereich dokumentieren

2.1.2 1.2 Referenzen

- **HIPAA Security Rule**: 45 CFR §§ 164.302-164.318
- **HIPAA Privacy Rule**: 45 CFR §§ 164.500-164.534
- **Breach Notification Rule**: 45 CFR §§ 164.400-164.414
- **HITECH Act**: Health Information Technology for Economic and Clinical Health Act
- **Omnibus Rule**: Abschließende Änderungen zu HIPAA (2013)

2.2 2. Organisationsinformationen

2.2.1 2.1 Organisationsdetails

Organisationsname: AdminSend GmbH
Adresse: Musterstraße 123, 80331 München
Bundesstaat: {{ meta.organization.state }}
Land: Deutschland
Website: https://www.adminsend.de
Steuer-ID (EIN): {{ meta.organization.tax_id }}

2.2.2 2.2 Organisationstyp

Primäre Klassifizierung: [TODO: Eine auswählen] - [ ] Covered Entity - Healthcare Provider (Gesundheitsdienstleister) - [ ] Covered Entity - Health Plan (Krankenversicherung) - [ ] Covered Entity - Healthcare Clearinghouse (Abrechnungsstelle) - [ ] Business Associate (Geschäftspartner) - [ ] Hybrid Entity (sowohl abgedeckte als auch nicht abgedeckte Funktionen)

Falls Healthcare Provider: - **Provider-Typ:** [TODO: Krankenhaus, Klinik, Arztpraxis, etc.] - **NPI (National Provider Identifier):** [TODO: 10-stellige NPI] - **Fachgebiete:** [TODO: Medizinische Fachgebiete auflisten] - **Elektronische Transaktionen:** [TODO: Ja/Nein - Übertragen Sie Gesundheitsinformationen elektronisch?]

Falls Health Plan: - **Plan-Typ:** [TODO: Gruppenkrankenversicherung, Krankenversicherer, HMO, Medicare, Medicaid, etc.] - **Anzahl der Teilnehmer:** [TODO: Anzahl] - **Small Health Plan:** [TODO: Ja/Nein - Weniger als 50 Teilnehmer]

Falls Healthcare Clearinghouse: - **Bereitgestellte Dienstleistungen:** [TODO: Anspruchsbearbeitung, Abrechnungsdienste, etc.] - **Betreute Covered Entities:** [TODO: Anzahl und Typen]

Falls Business Associate: - **Bereitgestellte Dienstleistungen:** [TODO: IT-Dienste, Abrechnung, Recht, Beratung, etc.] - **Covered Entity-Kunden:** [TODO: Anzahl] - **Subunternehmer:** [TODO: Ja/Nein]

2.2.3 2.3 Hybrid Entity-Bezeichnung

Ist dies eine Hybrid Entity? [TODO: Ja/Nein]

Falls ja, Folgendes ausfüllen:

Healthcare-Komponenten (Abgedeckte Funktionen): | Komponente | Funktion | Standort | PHI-Zugriff | |————|———-|———-|————-| | [TODO: Abteilung] | [TODO: Funktion] | [TODO: Standort] | [TODO: Ja/Nein] |

Nicht-Healthcare-Komponenten (Nicht abgedeckte Funktionen): | Komponente | Funktion | Standort | PHI-Zugriff | |————|———-|———-|————-| | [TODO: Abteilung] | [TODO: Funktion] | [TODO: Standort] | [TODO: Nein] |

Bezeichnungsdokumentation: [TODO: Verweis auf formale Hybrid Entity-Bezeichnung]

2.3 3. Protected Health Information (PHI)

2.3.1 3.1 PHI-Definition

Protected Health Information (PHI) umfasst individuell identifizierbare Gesundheitsinformationen, die: 1. Von einem Gesundheitsdienstleister, einer Krankenversicherung, einem Arbeitgeber oder einer Abrechnungsstelle erstellt oder empfangen wurden 2. Sich auf vergangene, gegenwärtige oder zukünftige körperliche oder geistige Gesundheit, Gesundheitsversorgung oder Zahlung für Gesundheitsversorgung beziehen 3. Die Person identifizieren oder zur Identifizierung der Person verwendet werden könnten

2.3.2 3.2 PHI-Elemente

Demografische Identifikatoren (18 HIPAA-Identifikatoren): 1. Namen 2. Geografische Unterteilungen kleiner als Bundesstaat (Straßenadresse, Stadt, Landkreis, Postleitzahl) 3. Daten (Geburt, Aufnahme, Entlassung, Tod) - außer Jahr 4. Telefonnummern 5. Faxnummern 6. E-Mail-Adressen 7. Sozialversicherungsnummern 8. Krankenakten-Nummern 9. Krankenversicherungs-Begünstigten-Nummern 10. Kontonummern 11. Zertifikats-/Lizenznummern 12. Fahrzeugkennzeichen und Seriennummern 13. Gerätekennzeichen und Seriennummern 14. Web-URLs 15. IP-Adressen 16. Biometrische Identifikatoren (Fingerabdrücke, Stimmabdrücke) 17. Ganzkörper-Fotografien 18. Jede andere eindeutige Identifikationsnummer, Merkmal oder Code

Gesundheitsinformationen: - Krankengeschichte und Diagnosen - Behandlungs- und Verfahrensinformationen - Medikamentenaufzeichnungen - Labor- und Testergebnisse - Versicherungs- und Abrechnungsinformationen - Klinische Notizen und Beurteilungen

2.3.3 3.3 PHI in der Organisation

Arten von gepflegten PHI: [TODO: Alle zutreffenden markieren] - [ ] Electronic PHI (ePHI) - elektronisch gespeichert - [ ] Paper PHI - physische Aufzeichnungen - [ ] Oral PHI - mündliche Kommunikation

Erfasste PHI-Datenelemente: | Datenelement | Format | Speicherort | Aufbewahrungsfrist | |———————|————|———————|————————-| | [TODO: Patientendemografie] | Elektronisch | [TODO: EHR-System] | [TODO: Jahre] | | [TODO: Krankenakten] | Elektronisch/Papier | [TODO: Standort] | [TODO: Jahre] | | [TODO: Abrechnungsinformationen] | Elektronisch | [TODO: System] | [TODO: Jahre] | | [TODO: Laborergebnisse] | Elektronisch | [TODO: System] | [TODO: Jahre] |

2.4 4. Systeme und Anwendungen

2.4.1 4.1 Systeme mit PHI

System-ID	Systemname	Typ	PHI-Elemente	Standort	Anbieter
[TODO: SYS-001]	[TODO: EHR-System]	Anwendung	Alle PHI	[TODO: On-Premise/Cloud]	[TODO: Anbieter]
[TODO: SYS-002]	[TODO: Praxisverwaltung]	Anwendung	Demografie, Abrechnung	[TODO: Standort]	[TODO: Anbieter]
[TODO: SYS-003]	[TODO: Laborsystem]	Anwendung	Laborergebnisse	[TODO: Standort]	[TODO: Anbieter]

System-ID	Systemname	Typ	PHI-Elemente	Standort	Anbieter
[TODO: SYS-004]	[TODO: Bildgebungssystem]	Anwendung	Radiologiebilder	[TODO: Standort]	[TODO: Anbieter]
[TODO: SYS-005]	[TODO: E-Mail-System]	Infrastruktur	PHI in Übertragung	[TODO: Standort]	[TODO: Anbieter]

2.4.2 4.2 Infrastrukturkomponenten

Komponente	Typ	Funktion	PHI-Zugriff	Standort
[TODO: DB-001]	Datenbankserver	PHI-Speicherung	Ja	[TODO: Rechenzentrum]
[TODO: APP-001]	Anwendungsserver	PHI-Verarbeitung	Ja	[TODO: Rechenzentrum]
[TODO: WEB-001]	Webserver	Patientenportal	Ja	[TODO: Cloud]
[TODO: FILE-001]	Dateiserver	Dokumentenspeicherung	Ja	[TODO: On-Premise]
[TODO: BACKUP-001]	Backup-System	PHI-Backup	Ja	[TODO: Standort]

2.4.3 4.3 Netzwerkarchitektur

Netzwerksegmente mit PHI: - **Klinisches Netzwerk:** [TODO: Beschreibung] - **Administratives Netzwerk:** [TODO: Beschreibung] - **DMZ:** [TODO: Beschreibung] - **Drahtlose Netzwerke:** [TODO: Beschreibung]

Netzwerkdiagramm: [TODO: Verweis auf Netzwerkdiagramm im diagrams/-Ordner]

2.5 5. Physische Standorte

2.5.1 5.1 Einrichtungen mit PHI

Standort-ID	Einrichtungsname	Adresse	Typ	PHI vorhanden	Mitarbeiteranzahl
[TODO: LOC-001]	Hauptklinik	[TODO: Adresse]	Klinisch	Ja	[TODO: Anzahl]
[TODO: LOC-002]	Verwaltungsbüro	[TODO: Adresse]	Administrativ	Ja	[TODO: Anzahl]
[TODO: LOC-003]	Rechenzentrum	[TODO: Adresse]	IT-Infrastruktur	Ja	[TODO: Anzahl]
[TODO: LOC-004]	Satellitenklinik	[TODO: Adresse]	Klinisch	Ja	[TODO: Anzahl]

2.5.2 5.2 Fernzugriff

Fernzugriff auf PHI erlaubt: [TODO: Ja/Nein]

Falls ja: - **Zugriffsmethode:** [TODO: VPN, Remote Desktop, Webportal] - **Authentifizierung:** [TODO: Benutzername/Passwort, MFA, Smart Card] - **Autorisierte Benutzer:** [TODO: Rollen/Anzahl] - **Geräte:** [TODO: Firmeneigene, BYOD, Beides] - **Mobile Device Management:** [TODO: Ja/Nein, Lösungsname]

2.6 6. Belegschaft

2.6.1 6.1 Belegschaft mit PHI-Zugriff

Rolle/Abteilung	Mitarbeiteranzahl	PHI-Zugriffsebene	Zugriffsbegründung
[TODO: Ärzte]	[TODO: Anzahl]	Vollständig	Direkte Patientenversorgung
[TODO: Pflegekräfte]	[TODO: Anzahl]	Vollständig	Direkte Patientenversorgung
[TODO: Medizinische Assistenten]	[TODO: Anzahl]	Eingeschränkt	Patientenaufnahme
[TODO: Abrechnungspersonal]	[TODO: Anzahl]	Nur Abrechnungsdaten	Anspruchsbearbeitung
[TODO: IT-Personal]	[TODO: Anzahl]	Systemadministration	Systemwartung
[TODO: Empfang]	[TODO: Anzahl]	Nur Demografie	Terminplanung

2.6.2 6.2 Belegschaftsschulung

HIPAA-Schulung erforderlich: Ja (Jährlich)
Schulungsthemen: - HIPAA Privacy Rule - HIPAA Security Rule - Breach Notification-Anforderungen - Organisationsrichtlinien und -verfahren - Sanktionen bei Verstößen

Aufbewahrung von Schulungsunterlagen: [TODO: Jahre]

2.7 7. Business Associates

2.7.1 7.1 Business Associate-Beziehungen

Business Associate	Bereitgestellte Dienstleistung	PHI-Zugriff	BAA unterzeichnet	BAA-Datum
[TODO: IT-Anbieter]	IT-Support	Ja	[TODO: Ja/Nein]	[TODO: Datum]
[TODO: Abrechnungsdienst]	Medizinische Abrechnung	Ja	[TODO: Ja/Nein]	[TODO: Datum]
[TODO: Cloud-Anbieter]	Daten-Hosting	Ja	[TODO: Ja/Nein]	[TODO: Datum]
[TODO: Aktenvernichtungsdienst]	Dokumentenvernichtung	Ja	[TODO: Ja/Nein]	[TODO: Datum]

Business Associate	Bereitgestellte Dienstleistung	PHI-Zugriff	BAA unterzeichnet	BAA-Datum
[TODO: Rechtsanwalt]	Rechtsdienstleistungen	Ja	[TODO: Ja/Nein]	[TODO: Datum]

2.7.2 7.2 Subunternehmer-Beziehungen

Nutzen Business Associates Subunternehmer? [TODO: Ja/Nein]

Falls ja: | Subunternehmer | Dienstleistung | Primärer BA | BAA vorhanden | |————————-|————————-|————————-|————————| | [TODO: Name] | [TODO: Dienstleistung] | [TODO: BA-Name] | [TODO: Ja/Nein] |

2.8 8. Compliance-Geltungsbereich

2.8.1 8.1 Anwendbare HIPAA-Regeln

Security Rule (45 CFR Part 164, Subpart C): [TODO: Anwendbar/Nicht anwendbar] - Administrative Safeguards (§164.308) - Physical Safeguards (§164.310) - Technical Safeguards (§164.312) - Organizational Requirements (§164.314) - Policies and Procedures (§164.316)

Privacy Rule (45 CFR Part 164, Subpart E): [TODO: Anwendbar/Nicht anwendbar] - Uses and Disclosures (§164.502-§164.514) - Individual Rights (§164.520-§164.528) - Administrative Requirements (§164.530-§164.534)

Breach Notification Rule (45 CFR Part 164, Subpart D): [TODO: Anwendbar/Nicht anwendbar] - Breach Discovery and Notification (§164.404-§164.410) - Notification by Business Associates (§164.410)

2.8.2 8.2 Ausschlüsse vom Geltungsbereich

Systeme/Prozesse NICHT im Geltungsbereich: | System/Prozess | Grund für Ausschluss | |————————-|————————-| | [TODO: HR-System] | Keine PHI - nur Mitarbeiterdaten | | [TODO: Marketing-Datenbank] | Nur de-identifizierte Daten | | [TODO: Öffentliche Website] | Keine PHI erfasst |

2.9 9. Compliance-Verantwortlichkeiten

2.9.1 9.1 Schlüsselrollen

Privacy Officer: - **Name:** {{ meta.roles.privacy_officer.name }} - **E-Mail:** {{ meta.roles.privacy_officer.email }} - **Telefon:** {{ meta.roles.privacy_officer.phone }}

Security Officer: - **Name:** {{ meta.roles.security_officer.name }} - **E-Mail:** {{ meta.roles.security_officer.email }} - **Telefon:** {{ meta.roles.security_officer.phone }}

HIPAA Compliance Officer: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

Kontaktperson (für Personen, die Rechte ausüben): - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon] - **Adresse:** [TODO: Postanschrift]

2.9.2 9.2 Governance-Struktur

HIPAA Compliance Committee: - **Vorsitz:** [TODO: Name, Titel] - **Mitglieder:** [TODO: Mitglieder und Titel auflisten] - **Sitzungshäufigkeit:** [TODO: Monatlich/Vierteljährlich] - **Verantwortlichkeiten:** Aufsicht über HIPAA-Compliance-Programm

2.10 10. Geltungsbereichsänderungen

2.10.1 10.1 Change Management-Prozess

Auslöser für Geltungsbereichsprüfung: 1. Neue Systeme oder Anwendungen, die PHI verarbeiten 2. Neue Business Associate-Beziehungen 3. Neue physische Standorte 4. Änderungen in bereitgestellten Dienstleistungen 5. Organisatorische Umstrukturierung 6. Regulatorische Änderungen

Prüfungsprozess: 1. Änderung identifizieren 2. HIPAA-Anwendbarkeit bewerten 3. Geltungsbereichsdokumentation aktualisieren 4. Erforderliche Schutzmaßnahmen implementieren 5. Richtlinien und Verfahren aktualisieren 6. Betroffene Belegschaft schulen 7. Änderungen dokumentieren

2.10.2 10.2 Geltungsbereichsprüfungsplan

Jährliche Prüfung: [TODO: Monat]
Letztes Prüfungsdatum: [TODO: Datum]
Nächstes Prüfungsdatum: [TODO: Datum]
Geprüft von: [TODO: Name, Titel]

2.10.3 10.3 Änderungshistorie

Datum	Änderungsbeschreibung	Auswirkung	Genehmigt durch
[TODO: Datum]	Initiale Geltungsbereichsdefinition	N/A	[TODO: Name]
[TODO: Datum]	Neues EHR-System hinzugefügt	Erweiterter ePHI-Geltungsbereich	[TODO: Name]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 3

Covered Entities und Healthcare-Komponenten

Dokument-ID: HIPAA-0020
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

3.1 1. Zweck

Dieses Dokument definiert den Status von AdminSend GmbH als HIPAA Covered Entity und dokumentiert alle Healthcare-Komponenten und abgedeckten Funktionen.

3.1.1 1.1 Zielsetzungen

- **Entity-Klassifizierung:** Organisationsstatus unter HIPAA klar definieren
- **Komponentenidentifizierung:** Alle Healthcare-Komponenten dokumentieren (falls Hybrid Entity)
- **Funktionsdokumentation:** Alle abgedeckten Funktionen und Aktivitäten auflisten
- **Compliance-Grenzen:** Klare Grenzen für HIPAA-Compliance festlegen

3.2 2. Covered Entity-Bestimmung

3.2.1 2.1 Covered Entity-Definition

Unter HIPAA ist eine Covered Entity: 1. **Healthcare Provider** (Gesundheitsdienstleister), der bestimmte Transaktionen elektronisch durchführt 2. **Health Plan** (Krankenversicherung), der medizinische Versorgung bereitstellt oder bezahlt 3. **Healthcare Clearinghouse** (Abrechnungsstelle), das Gesundheitsinformationen verarbeitet

3.2.2 2.2 Organisationsklassifizierung

AdminSend GmbH ist ein: [TODO: Eine auswählen]

- ☐ **Healthcare Provider** (45 CFR §160.103)
- ☐ **Health Plan** (45 CFR §160.103)
- ☐ **Healthcare Clearinghouse** (45 CFR §160.103)
- ☐ **Hybrid Entity** (45 CFR §164.105(a))

Klassifizierungsbegründung: [TODO: Erklären, warum die Organisation die Covered Entity-Definition erfüllt]

3.3 3. Healthcare Provider-Details

Diesen Abschnitt ausfüllen, falls die Organisation ein Healthcare Provider ist

3.3.1 3.1 Provider-Informationen

Provider-Typ: [TODO: Zutreffendes auswählen] - [ ] Krankenhaus - [ ] Arztpraxis - [ ] Klinik - [ ] Pflegeheim - [ ] Apotheke - [ ] Labor - [ ] Rettungsdienst - [ ] Sonstiges: [TODO: Angeben]

National Provider Identifier (NPI): - **NPI-Nummer:** [TODO: 10-stellige NPI] - **NPI-Typ:** [TODO: Typ 1 (Individuell) oder Typ 2 (Organisation)] - **Registrierungsdatum:** [TODO: Datum]

Medizinische Fachgebiete: | Fachgebiet | Taxonomie-Code | Anbieter | |————|————-|————-| | [TODO: Allgemeinmedizin] | [TODO: Code] | [TODO: Anzahl] | | [TODO: Fachgebiet 1] | [TODO: Code] | [TODO: Anzahl] | | [TODO: Fachgebiet 2] | [TODO: Code] | [TODO: Anzahl] |

3.3.2 3.2 Elektronische Transaktionen

Überträgt die Organisation Gesundheitsinformationen elektronisch im Zusammenhang mit einer HIPAA-Standardtransaktion? [TODO: Ja/Nein]

Durchgeführte HIPAA-Standardtransaktionen: - [ ] Gesundheitsansprüche oder gleichwertige Begegnungsinformationen (837) - [ ] Berechtigung für einen Gesundheitsplan (270/271) - [ ] Überweisungszertifizierung und -autorisierung (278) - [ ] Gesundheitsanspruchsstatus (276/277) - [ ] Anmeldung und Abmeldung bei einem Gesundheitsplan (834) - [ ] Gesundheitszahlung und Überweisungsberatung (835) - [ ] Gesundheitsplan-Prämienzahlungen (820) - [ ] Koordination der Leistungen (837)

Transaktionsvolumen (Jährlich): | Transaktionstyp | Volumen | Primärer Handelspartner | |————————|———|————————-| | [TODO: Ansprüche] | [TODO: Anzahl] | [TODO: Zahler-Name] | | [TODO: Berechtigung] | [TODO: Anzahl] | [TODO: Zahler-Name] |

3.3.3 3.3 Bereitgestellte Gesundheitsdienstleistungen

Angebotene Dienstleistungen: | Dienstleistung | Beschreibung | Standort | PHI generiert | |—————-|—————|———-|—————| | [TODO: Allgemeinmedizin] | [TODO: Beschreibung] | [TODO: Standort] | Ja | | [TODO: Diagnostische Dienste] | [TODO: Beschreibung] | [TODO: Standort] | Ja | | [TODO: Behandlungsdienste] | [TODO: Beschreibung] | [TODO: Standort] | Ja |

3.4 4. Health Plan-Details

Diesen Abschnitt ausfüllen, falls die Organisation ein Health Plan ist

3.4.1 4.1 Health Plan-Informationen

Plan-Typ: [TODO: Zutreffendes auswählen] - [ ] Gruppenkrankenversicherung - [ ] Krankenversicherer - [ ] HMO (Health Maintenance Organization) - [ ] Medicare - [ ] Medicaid - [ ] Medicare Advantage - [ ] Medicare Part D - [ ] TRICARE - [ ] Sonstiges: [TODO: Angeben]

Plan-Merkmale: - **Anzahl der Teilnehmer:** [TODO: Anzahl] - **Small Health Plan:** [TODO: Ja/Nein - Weniger als 50 Teilnehmer] - **Selbstversichert:** [TODO: Ja/Nein] - **Vollversichert:** [TODO: Ja/Nein]

Plan-Sponsor-Informationen: - **Sponsor-Name:** [TODO: Name] - **Sponsor-Typ:** [TODO: Arbeitgeber, Gewerkschaft, etc.] - **Beziehung zum Plan:** [TODO: Beschreibung]

3.4.2 4.2 Health Plan-Funktionen

Durchgeführte Funktionen: - [ ] Anspruchsbearbeitung - [ ] Berechtigungsbestimmung - [ ] Anmeldung und Abmeldung - [ ] Prämieneinzug - [ ] Anbieternetzwerkverwaltung - [ ] Nutzungsüberprüfung - [ ] Fallmanagement - [ ] Krankheitsmanagement

PHI verwendet für: - [ ] Zahlung - [ ] Gesundheitsbetrieb - [ ] Behandlungskoordination - [ ] Qualitätsverbesserung - [ ] Betrugserkennung

3.5 5. Healthcare Clearinghouse-Details

Diesen Abschnitt ausfüllen, falls die Organisation ein Healthcare Clearinghouse ist

3.5.1 5.1 Clearinghouse-Informationen

Bereitgestellte Dienstleistungen: - [ ] Anspruchsbearbeitung - [ ] Anspruchsbereinigung - [ ] Formatkonvertierung - [ ] Transaktionsweiterleitung - [ ] Berechtigungsüberprüfung - [ ] Sonstiges: [TODO: Angeben]

Betreute Covered Entities: - **Anzahl der Anbieter:** [TODO: Anzahl] - **Anzahl der Zahler:** [TODO: Anzahl] - **Transaktionsvolumen (Monatlich):** [TODO: Anzahl]

Unterstützte Standardformate: | Transaktion | Format | Version | |————————-|———|————| | [TODO: Ansprüche] | X12 837 | [TODO: 5010] | | [TODO: Berechtigung] | X12 270/271 | [TODO: 5010] |

3.6 6. Hybrid Entity-Bezeichnung

Diesen Abschnitt ausfüllen, falls die Organisation eine Hybrid Entity ist

3.6.1 6.1 Hybrid Entity-Definition

Eine Hybrid Entity ist eine Organisation, die: 1. Sowohl abgedeckte als auch nicht abgedeckte Funktionen ausführt 2. Ihre Healthcare-Komponenten formal bezeichnet hat 3. HIPAA nur auf

bezeichnete Healthcare-Komponenten anwendet

Ist AdminSend GmbH eine Hybrid Entity? [TODO: Ja/Nein]

3.6.2 6.2 Healthcare-Komponenten

Bezeichnete Healthcare-Komponenten:

Komponenten-ID	Komponentenname	Funktion	Standort	Mitarbeiteranzahl
[TODO: HC-001]	[TODO: Medizinische Klinik]	Healthcare Provider	[TODO: Gebäude A]	[TODO: 25]
[TODO: HC-002]	[TODO: Mitarbeiter-Gesundheitsplan]	Health Plan	[TODO: HR-Abteilung]	[TODO: 5]
[TODO: HC-003]	[TODO: Arbeitsmedizin]	Healthcare Provider	[TODO: Gebäude B]	[TODO: 10]

Healthcare-Komponentenfunktionen: | Komponente | Abgedeckte Funktionen | Erstellte/Gepflegte PHI | |————|————————-|————————-| | [TODO: Medizinische Klinik] | Patientenversorgung, Abrechnung | Patientenakten, Abrechnungsdaten | | [TODO: Mitarbeiter-Gesundheitsplan] | Anspruchsbearbeitung | Ansprüche, Anmeldedaten |

3.6.3 6.3 Nicht-Healthcare-Komponenten

Nicht abgedeckte Komponenten:

Komponenten-ID	Komponentenname	Funktion	PHI-Zugriff
[TODO: NC-001]	[TODO: Fertigung]	Produktherstellung	Nein
[TODO: NC-002]	[TODO: Vertrieb]	Produktverkauf	Nein
[TODO: NC-003]	[TODO: Unternehmens-IT]	IT-Support (nicht Healthcare)	Nein

Begründung für nicht abgedeckten Status: [TODO: Erklären, warum diese Komponenten keine abgedeckten Funktionen sind]

3.6.4 6.4 Hybrid Entity-Dokumentation

Formales Bezeichnungsdokument: - **Dokumenttitel:** [TODO: “Hybrid Entity-Bezeichnung”] - **Bezeichnungsdatum:** [TODO: Datum] - **Genehmigt durch:** [TODO: Vorstand, CEO, etc.] - **Dokumentstandort:** [TODO: Dateipfad oder Verweis]

Bezeichnungskriterien: - Klare Trennung abgedeckter und nicht abgedeckter Funktionen - Separate Verwaltung und Betrieb - Unterschiedliche Belegschaftszuweisungen - Separate physische Standorte (falls zutreffend)

3.6.5 6.5 Belegschaftszuweisung

Healthcare-Komponenten-Belegschaft: | Mitarbeiter-ID | Name | Rolle | Komponente | PHI-Zugriff | |————————-|——|——|———|————-| | [TODO: EMP-001] | [TODO: Name] | [TODO: Arzt] | HC-001 | Vollständig | | [TODO: EMP-002] | [TODO: Name] | [TODO: Pflegekraft] | HC-001 | Vollständig | | [TODO: EMP-003] | [TODO: Name] | [TODO: Anspruchsbearbeiter] | HC-002 | Eingeschränkt |

Gemeinsame Belegschaft: | Mitarbeiter-ID | Name | Rolle | Zugriff auf Healthcare-Komponenten | |————————-|——|——|———————————| | [TODO: EMP-100] | [TODO: Name] | [TODO: IT-Support] | HC-001, HC-002 (nur Systemadministration) | | [TODO: EMP-101] | [TODO: Name] | [TODO: Recht] | Alle Komponenten (nach Bedarf) |

Belegschaftsschulung: - Healthcare-Komponenten-Belegschaft: Vollständige HIPAA-Schulung - Gemeinsame Belegschaft: HIPAA-Schulung für Healthcare-Komponentenzugriff - Nicht-Healthcare-Belegschaft: Keine HIPAA-Schulung erforderlich (außer bei PHI-Zugriff)

3.7 7. Abgedeckte Funktionen

3.7.1 7.1 Healthcare Operations

Durchgeführte Healthcare Operations: - [ ] Qualitätsbewertung und -verbesserung - [ ] Fallmanagement und Versorgungskoordination - [ ] Überprüfung der Kompetenz von Gesundheitsfachkräften - [ ] Underwriting und Prämienbewertung (Gesundheitspläne) - [ ] Medizinische Überprüfung und Nutzungsüberprüfung - [ ] Betrugs- und Missbrauchserkennung - [ ] Geschäftsplanung und -entwicklung - [ ] Geschäftsführung und allgemeine Verwaltungsaktivitäten

Für Healthcare Operations verwendete PHI: | Operation | Verwendete PHI-Elemente | Häufigkeit | Verantwortliche Abteilung | |————|———————|————|———————————| | [TODO: Qualitätsverbesserung] | [TODO: Klinische Daten] | [TODO: Vierteljährlich] | [TODO: Qualitätsabteilung] | | [TODO: Nutzungsüberprüfung] | [TODO: Anspruchsdaten] | [TODO: Laufend] | [TODO: UM-Abteilung] |

3.7.2 7.2 Behandlungsaktivitäten

Behandlungsfunktionen: - [ ] Bereitstellung von Gesundheitsdienstleistungen - [ ] Versorgungskoordination - [ ] Patientenüberweisung - [ ] Konsultation zwischen Anbietern - [ ] Fallmanagement

Behandlungsstandorte: | Standort | Dienstleistungen | Anbieter | Patientenvolumen | |————-|———————|————-|——————| | [TODO: Hauptklinik] | [TODO: Allgemeinmedizin] | [TODO: 5 Ärzte] | [TODO: 100/Tag] | | [TODO: Satellitenbüro] | [TODO: Fachversorgung] | [TODO: 2 Spezialisten] | [TODO: 30/Tag] |

3.7.3 7.3 Zahlungsaktivitäten

Zahlungsfunktionen: - [ ] Abrechnung und Anspruchsverwaltung - [ ] Anspruchsbearbeitung - [ ] Zahlungseinzug - [ ] Erstattung - [ ] Nutzungsüberprüfung für Zahlung - [ ] Vorautorisierung

Zahlungssysteme: | System | Funktion | Verarbeitete PHI | Volumen | |———|————-|———————|————| | [TODO: Abrechnungssystem] | Anspruchserstellung | Abrechnungsdaten | [TODO: 500/Tag] | | [TODO: Zahlungsportal] | Patientenzahlungen | Demografie, Konto | [TODO: 100/Tag] |

3.8 8. Compliance-Auswirkungen

3.8.1 8.1 Anwendbarkeit der HIPAA-Regeln

Für Covered Entity: - **Privacy Rule:** Gilt für alle PHI - **Security Rule:** Gilt für alle ePHI - **Breach Notification Rule:** Gilt für alle ungesicherten PHI

Für Hybrid Entity: - **Privacy Rule:** Gilt nur für Healthcare-Komponenten - **Security Rule:** Gilt nur für Healthcare-Komponenten - **Breach Notification Rule:** Gilt nur für Healthcare-Komponenten - **Hinweis:** Gemeinsame Belegschaft und Infrastruktur müssen beim Zugriff auf Healthcare-Komponenten-PHI konform sein

3.8.2 8.2 Dokumentationsanforderungen

Erforderliche Dokumentation: - [ ] Covered Entity-Bestimmung - [ ] Hybrid Entity-Bezeichnung (falls zutreffend) - [ ] Healthcare-Komponentendefinitionen - [ ] Belegschaftszuweisungen - [ ] Business Associate Agreements - [ ] Richtlinien und Verfahren - [ ] Schulungsunterlagen

Dokumentationsaufbewahrung: [TODO: 6 Jahre ab Erstellung oder letztem Gültigkeitsdatum]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated | default('') }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 4

Business Associates und Subunternehmer

Dokument-ID: HIPAA-0030
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

4.1 1. Zweck

Dieses Dokument identifiziert und verwaltet alle Business Associate-Beziehungen für AdminSend GmbH und stellt die Einhaltung der HIPAA Business Associate-Anforderungen sicher.

4.1.1 1.1 Zielsetzungen

- **BA-Identifikation:** Alle Entitäten identifizieren, die die Business Associate-Definition erfüllen
- **BAA-Verwaltung:** Sicherstellen, dass gültige Business Associate Agreements vorhanden sind
- **Compliance-Überwachung:** BA-Compliance mit HIPAA-Anforderungen überwachen
- **Subunternehmer-Aufsicht:** Subunternehmer-Beziehungen verfolgen und verwalten

4.1.2 1.2 Referenzen

- **HIPAA Privacy Rule**: 45 CFR §164.502(e), §164.504(e)
- **HIPAA Security Rule**: 45 CFR §164.308(b)
- **HIPAA Breach Notification Rule**: 45 CFR §164.410
- **HITECH Act**: Business Associate-Haftungsbestimmungen

4.2 2. Business Associate-Definition

4.2.1 2.1 Was ist ein Business Associate?

Ein Business Associate ist eine Person oder Entität, die: 1. Funktionen oder Aktivitäten im Namen einer Covered Entity ausführt oder Dienstleistungen für diese erbringt 2. Die Nutzung oder Offenlegung von PHI beinhaltet 3. Nicht Teil der Belegschaft der Covered Entity ist

4.2.2 2.2 Häufige Business Associate-Funktionen

Business Associate-Dienstleistungen umfassen: - Anspruchsbearbeitung oder -verwaltung - Datenanalyse, -verarbeitung oder -verwaltung - Nutzungsüberprüfung - Qualitätssicherung - Abrechnung, Leistungsverwaltung, Praxisverwaltung - Neubepreisungsdienste oder andere Dienstleistungen - Rechts-, versicherungsmathematische, buchhalterische, beratende, Datenaggregations-, Verwaltungs-, administrative, Akkreditierungs- oder Finanzdienstleistungen

Beispiele für Business Associates: - Drittverwalter - Abrechnungsunternehmen - IT-Dienstleister (mit PHI-Zugriff) - Cloud-Speicheranbieter - Aktenvernichtungsunternehmen - Rechtsanwälte (mit PHI-Zugriff) - Berater (mit PHI-Zugriff) - Datenanalysefirmen

4.2.3 2.3 Entitäten, die KEINE Business Associates sind

Conduit-Ausnahme: - Telekommunikationsunternehmen - Internet Service Provider (ISPs) - Postdienste - Kurierdienste (wenn nur versiegelte PHI transportiert wird)

Andere Ausnahmen: - Belegschaftsmitglieder - Gesundheitsdienstleister in Behandlungsbeziehung - Krankenversicherungsmitglieder - Gruppenkrankenversicherungs-Sponsoren (mit bestimmten Einschränkungen)

4.3 3. Business Associate-Inventar

4.3.1 3.1 Aktuelle Business Associates

BA-ID	Business Associate-Name	Bereitgestellte Dienstleistung	PHI-Zugriffstyp	BAA-Status	BAA-Datum	Prüfungsdatum
[TODO: BA-001]	[TODO: IT-Support-Anbieter]	IT-Support und -Wartung	ePHI-Zugriff	[TODO: Aktiv]	[TODO: 2024-01-15]	[TODO: 2027-01-15]
[TODO: BA-002]	[TODO: Abrechnungsdienst]	Medizinische Abrechnung	PHI-Verarbeitung	[TODO: Aktiv]	[TODO: 2023-06-01]	[TODO: 2026-06-01]
[TODO: BA-003]	[TODO: Cloud-Anbieter]	Daten-Hosting	ePHI-Speicherung	[TODO: Aktiv]	[TODO: 2025-03-10]	[TODO: 2028-03-10]

4.3.2 3.2 Business Associate-Details

BA-001: [TODO: IT-Support-Anbieter] - **Kontaktperson:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon] - **Adresse:** [TODO: Adresse] - **Dienstleis-**

tungen: [TODO: Detaillierte Beschreibung] - **PHI-Zugriff:** [TODO: Zugriffssysteme, Zugriffstyp] - **Subunternehmer:** [TODO: Ja/Nein, auflisten falls ja] - **Versicherung:** [TODO: Cyber-Haftpflichtdeckung Betrag] - **Compliance-Bestätigung:** [TODO: Datum der letzten Bestätigung]

4.4 4. Business Associate Agreements (BAAs)

4.4.1 4.1 BAA-Anforderungen

Erforderliche BAA-Bestimmungen (45 CFR §164.504(e)):

1. **Zulässige Nutzungen und Offenlegungen:**
   - Zulässige Nutzungen und Offenlegungen von PHI spezifizieren
   - Nutzungen/Offenlegungen auf vertraglich oder gesetzlich erforderliche beschränken
2. **Schutzmaßnahmen:**
   - Angemessene Schutzmaßnahmen zur Verhinderung unbefugter Nutzung/Offenlegung implementieren
   - Security Rule für ePHI einhalten
3. **Subunternehmer-Anforderungen:**
   - Sicherstellen, dass Subunternehmer denselben Beschränkungen zustimmen
   - Zufriedenstellende Zusicherungen von Subunternehmern einholen
4. **Berichterstattung:**
   - Unbefugte Nutzungen/Offenlegungen an Covered Entity melden
   - Sicherheitsvorfälle melden
   - Verstöße gegen ungesicherte PHI melden
5. **Individuelle Rechte:**
   - PHI für Zugriffsanfragen verfügbar machen
   - PHI für Änderungsanfragen verfügbar machen
   - Rechenschaft über Offenlegungen ablegen
6. **Compliance:**
   - Interne Praktiken, Bücher und Aufzeichnungen für HHS-Compliance-Prüfung verfügbar machen
   - PHI bei Beendigung zurückgeben oder vernichten (falls machbar)
7. **Beendigung:**
   - Beendigung autorisieren, wenn BA wesentliche Bedingung verletzt
   - PHI-Disposition bei Beendigung spezifizieren

4.4.2 4.2 BAA-Vorlage

Standard-BAA-Vorlagenstandort: [TODO: Dateipfad oder Dokumentenmanagementsystem-Standort]

BAA-Vorlagenversion: [TODO: Versionsnummer und Datum]

Vorlagengenehmigung: - **Genehmigt durch Rechtsabteilung:** [TODO: Ja/Nein, Datum] - **Genehmigt durch Privacy Officer:** [TODO: Ja/Nein, Datum] - **Genehmigt durch Compliance:** [TODO: Ja/Nein, Datum]

4.4.3 4.3 BAA-Ausführungsprozess

Prozessschritte: 1. Bedarf für Business Associate-Beziehung identifizieren 2. BA-Due-Diligence und Risikobewertung durchführen 3. Dienstleistungsvereinbarung aushandeln 4. Business Associate Agreement ausführen 5. BAA im Inventar dokumentieren 6. BA-Compliance überwachen 7. BAA regelmäßig überprüfen (mindestens alle 3 Jahre)

Genehmigungsbefugnis: - **Dienstleistungen < 10.000 $:** [TODO: Abteilungsleiter] - **Dienstleistungen 10.000-50.000 $:** [TODO: Direktor + Privacy Officer] - **Dienstleistungen > 50.000 $:** [TODO: Geschäftsführung + Privacy Officer + Rechtsabteilung]

4.5 5. Subunternehmer-Verwaltung

4.5.1 5.1 Subunternehmer-Anforderungen

HIPAA-Anforderungen für Subunternehmer: - Business Associates müssen zufriedenstellende Zusicherungen von Subunternehmern einholen - Subunternehmer müssen BAA mit Business Associate abschließen - Subunternehmer haben dieselben HIPAA-Verpflichtungen wie Business Associates - Covered Entity muss über Subunternehmer-Vereinbarungen benachrichtigt werden

4.5.2 5.2 Subunternehmer-Inventar

Subunternehmer	Primärer BA	Dienstleistung	PHI-Zugriff	BAA mit BA	CE benachrichtigt
[TODO: Cloud-Backup-Anbieter]	[TODO: IT-Anbieter]	Datensicherung	ePHI	[TODO: Ja]	[TODO: Ja, Datum]
[TODO: Offshore-Support]	[TODO: IT-Anbieter]	Help Desk	ePHI	[TODO: Ja]	[TODO: Ja, Datum]

4.5.3 5.3 Subunternehmer-Genehmigungsprozess

Covered Entity-Genehmigung erforderlich: [TODO: Ja/Nein]

Genehmigungsprozess: 1. Business Associate beantragt Genehmigung zur Nutzung von Subunternehmern 2. BA stellt Subunternehmer-Informationen und vorgeschlagenes BAA bereit 3. Privacy Officer prüft Subunternehmer-Vereinbarung 4. Genehmigung erteilt oder abgelehnt innerhalb [TODO: 10 Werktage] 5. BA führt BAA mit Subunternehmer aus 6. BA stellt Kopie des ausgeführten BAA an Covered Entity bereit

4.6 6. Business Associate Due Diligence

4.6.1 6.1 Bewertung vor Vertragsabschluss

Due Diligence-Checkliste: - [ ] Business Associate-Fragebogen ausgefüllt - [ ] HIPAA-Compliance-Bestätigung erhalten - [ ] Sicherheitskontroll-Dokumentation geprüft - [ ] Incident Response-Plan geprüft - [ ] Breach Notification-Verfahren geprüft - [ ] Versicherungsschutz

verifiziert (Cyber-Haftpflicht) - [ ] Referenzen geprüft - [ ] Finanzielle Stabilität bewertet - [ ] Subunternehmer-Liste bereitgestellt

Risikobewertung: | Risikofaktor | Bewertung | Minderung | |————-|————|————| | [TODO: Datenvolumen] | [TODO: Hoch/Mittel/Niedrig] | [TODO: Minderungsmaßnahmen] | | [TODO: PHI-Sensibilität] | [TODO: Hoch/Mittel/Niedrig] | [TODO: Minderungsmaßnahmen] | | [TODO: Sicherheitsreife] | [TODO: Hoch/Mittel/Niedrig] | [TODO: Minderungsmaßnahmen] |

4.6.2 6.2 Laufende Überwachung

Überwachungsaktivitäten: - Jährliche Compliance-Bestätigung - Regelmäßige Sicherheitsbewertungen - Breach Notification-Verfolgung - Vorfallsprüfung - Leistungsüberprüfungen - Vertragskonformitätsprüfungen

Überwachungsplan: | Aktivität | Häufigkeit | Verantwortliche Partei | Zuletzt abgeschlossen | |————-|————|————————|———————-| | [TODO: Compliance-Bestätigung] | Jährlich | [TODO: Privacy Officer] | [TODO: Datum] | | [TODO: Sicherheitsbewertung] | Jährlich | [TODO: Security Officer] | [TODO: Datum] | | [TODO: Leistungsüberprüfung] | Vierteljährlich | [TODO: Vertragsmanager] | [TODO: Datum] |

4.7 7. Breach Notification von Business Associates

4.7.1 7.1 BA Breach Notification-Anforderungen

Business Associates müssen Covered Entity benachrichtigen: - **Zeitrahmen:** Ohne unangemessene Verzögerung, spätestens 60 Tage nach Entdeckung - **Methode:** Schriftliche Benachrichtigung (E-Mail akzeptabel) - **Inhalt:** - Identifizierung jeder betroffenen Person - Beschreibung des Verstoßes - Arten der beteiligten PHI - Datum des Verstoßes und Entdeckungsdatum - Schritte, die Personen unternehmen sollten - Untersuchungs- und Minderungsbemühungen des BA

4.7.2 7.2 Breach Notification-Protokoll

Verstoß-ID	BA-Name	Entdeckungsdatum	Benachrichtigungsdatum	Betroffene Personen	Beteiligte PHI	Status
[TODO: BR-001]	[TODO: BA-Name]	[TODO: Datum]	[TODO: Datum]	[TODO: Anzahl]	[TODO: Typen]	[TODO: Gelöst]

4.7.3 7.3 Breach Response-Prozess

Bei Erhalt einer BA Breach Notification: 1. Empfang der Benachrichtigung bestätigen 2. Bei Bedarf zusätzliche Informationen anfordern 3. Verstoß auf Meldepflichten bewerten 4. Betroffene Personen benachrichtigen (falls erforderlich) 5. HHS benachrichtigen (falls erforderlich) 6. Medien benachrichtigen (falls erforderlich - 500+ Personen) 7. Verstoß und Reaktion dokumentieren 8. BA-Beziehung und Kontrollen überprüfen

4.8 8. Business Associate-Beendigung

4.8.1 8.1 Beendigungsauslöser

Gründe für Beendigung: - Wesentlicher Verstoß gegen BAA - Versäumnis, Verstoß innerhalb festgelegter Frist zu beheben - Wiederholte Sicherheitsvorfälle - Versäumnis, Verstöße zu melden - Insolvenz oder Konkurs - Ende der Dienstleistungsbeziehung

4.8.2 8.2 Beendigungsprozess

Beendigungsschritte: 1. Schriftliche Beendigungsmitteilung bereitstellen 2. Beendigungsdatum angeben 3. Rückgabe oder Vernichtung von PHI anfordern 4. PHI-Rückgabe/-Vernichtung verifizieren 5. Vernichtungszertifikat einholen (falls zutreffend) 6. Business Associate-Inventar aktualisieren 7. Betroffene Systeme/Abteilungen benachrichtigen 8. Nachbeendigungsprüfung durchführen

4.8.3 8.3 PHI-Disposition

Optionen bei Beendigung: - **PHI zurückgeben:** BA gibt alle PHI an Covered Entity zurück - **PHI vernichten:** BA vernichtet PHI und stellt Zertifikat bereit - **PHI aufbewahren:** Falls Rückgabe/Vernichtung nicht machbar, behält BA PHI mit fortgesetztem Schutz

Aufbewahrungsbegründung: [TODO: Gründe dokumentieren, falls PHI-Aufbewahrung erforderlich ist]

4.9 9. Compliance und Audit

4.9.1 9.1 BA-Compliance-Überwachung

Überwachungsmethoden: - Jährliche Compliance-Bestätigungen - Vor-Ort-Audits (falls vertraglich gestattet) - Sicherheitsbewertungen - Penetrationstestergebnisse-Prüfung - SOC 2-Berichte-Prüfung - ISO 27001-Zertifizierungen-Prüfung

Audit-Rechte: - Covered Entity behält sich das Recht vor, BA-Compliance zu prüfen - Audit-Häufigkeit: [TODO: Jährlich oder nach Bedarf] - Audit-Umfang: HIPAA-Compliance, Sicherheitskontrollen, BAA-Compliance

4.9.2 9.2 Dokumentation und Aufzeichnungen

Erforderliche Dokumentation: - Ausgeführte Business Associate Agreements - Due Diligence-Bewertungen - Compliance-Bestätigungen - Breach Notifications - Audit-Berichte - Korrespondenz bezüglich PHI

Aufbewahrungsfrist: [TODO: 6 Jahre ab Erstellung oder letztem Gültigkeitsdatum]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 5

Rollen und Verantwortlichkeiten

Dokument-ID: HIPAA-0040
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

5.1 1. Zweck

Dieses Dokument definiert die Rollen, Verantwortlichkeiten und Zuständigkeiten für die HIPAA-Compliance bei AdminSend GmbH.

5.1.1 1.1 Zielsetzungen

- **Rollendefinition:** HIPAA-erforderliche und unterstützende Rollen klar definieren
- **Verantwortlichkeit:** Entscheidungsbefugnisse festlegen
- **Compliance:** HIPAA-Anforderungen für benannte Beauftragte erfüllen
- **Kommunikation:** Klare Kommunikations- und Eskalationswege etablieren

5.1.2 1.2 HIPAA-erforderliche Rollen

HIPAA-Mandate: - **Privacy Officer** (45 CFR §164.530(a)(1)(i)) - Erforderlich - **Security Officer** (45 CFR §164.308(a)(2)) - Erforderlich - **Kontaktperson** für individuelle Rechte (45 CFR §164.530(a)(1)(ii)) - Erforderlich

5.2 2. Geschäftsführung

5.2.1 2.1 Chief Executive Officer (CEO)

Name: {{ meta.roles.ceo.name }}
E-Mail: {{ meta.roles.ceo.email }}
Telefon: {{ meta.roles.ceo.phone }}

Verantwortlichkeiten: - Ultimative Verantwortung für HIPAA-Compliance - Genehmigung von HIPAA-Richtlinien und -Verfahren - Ressourcenzuweisung für Compliance-Programm - Aufsicht über Privacy und Security Officers - Finale Eskalationsstelle für Compliance-Fragen - Genehmigung von Sanktionen bei Richtlinienverstößen

5.2.2 2.2 Chief Information Officer (CIO)

Name: {{ meta.roles.cio.name }}
E-Mail: {{ meta.roles.cio.email }}
Telefon: {{ meta.roles.cio.phone }}

Verantwortlichkeiten: - IT-Infrastruktur zur Unterstützung der HIPAA-Compliance - Technologieinvestitionen für Sicherheit und Datenschutz - Aufsicht über Security Officer - Genehmigung technischer Schutzmaßnahmen - IT-Risikomanagement

5.3 3. HIPAA-erforderliche Rollen

5.3.1 3.1 Privacy Officer

Name: {{ meta.roles.privacy_officer.name }}
E-Mail: {{ meta.roles.privacy_officer.email }}
Telefon: {{ meta.roles.privacy_officer.phone }}
Bürostandort: [TODO: Standort]

HIPAA-Anforderung: 45 CFR §164.530(a)(1)(i)

Verantwortlichkeiten: - Entwicklung und Implementierung von Datenschutzrichtlinien und -verfahren - Verwaltung des Datenschutz-Schulungsprogramms - Untersuchung von Datenschutzbeschwerden - Datenschutz-Incident-Response - Bearbeitung individueller Rechtsanfragen (Zugriff, Änderung, Rechenschaftspflicht) - Aufsicht über Business Associate Agreements - Datenschutz-Risikobewertungen - Pflege der Notice of Privacy Practices - Datenschutz-Compliance-Überwachung - Verbindung zum HHS Office for Civil Rights (OCR)

Befugnisse: - Zugriff auf alle PHI und Systeme - Befugnis zur Untersuchung von Datenschutzangelegenheiten - Empfehlung von Sanktionen bei Datenschutzverstößen - Genehmigung datenschutzbezogener Richtlinien - Stoppen von Aktivitäten, die Datenschutzanforderungen verletzen

Backup Privacy Officer: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

5.3.2 3.2 Security Officer

Name: {{ meta.roles.security_officer.name }}
E-Mail: {{ meta.roles.security_officer.email }}
Telefon: {{ meta.roles.security_officer.phone }}
Bürostandort: [TODO: Standort]

HIPAA-Anforderung: 45 CFR §164.308(a)(2)

Verantwortlichkeiten: - Entwicklung und Implementierung von Sicherheitsrichtlinien und -verfahren - Sicherheitsrisikoanalyse und Risikomanagement - Verwaltung des Sicherheits-Schulungsprogramms - Sicherheits-Incident-Response - Implementierung technischer, physischer und administrativer Schutzmaßnahmen - Zugriffskontrollverwaltung - Audit-Log-Überprüfung und -Überwachung - Schwachstellenmanagement - Sicherheits-Compliance-Überwachung - Verbindung zu Sicherheitsanbietern und -beratern

Befugnisse: - Zugriff auf alle Systeme und Sicherheitskontrollen - Befugnis zur Untersuchung von Sicherheitsvorfällen - Empfehlung von Sanktionen bei Sicherheitsverstößen - Genehmigung sicherheitsbezogener Richtlinien - Notfallbefugnis zum Deaktivieren von Zugriff oder Systemen

Backup Security Officer: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

5.3.3 3.3 Kontaktperson für individuelle Rechte

Name: [TODO: Name]
E-Mail: [TODO: E-Mail]
Telefon: [TODO: Telefon]
Postanschrift: [TODO: Adresse]

HIPAA-Anforderung: 45 CFR §164.530(a)(1)(ii)

Verantwortlichkeiten: - Empfang und Bearbeitung von Anfragen auf Zugriff auf PHI - Empfang und Bearbeitung von Anfragen auf Änderung von PHI - Empfang und Bearbeitung von Anfragen auf Rechenschaftspflicht über Offenlegungen - Empfang und Bearbeitung von Anfragen auf Einschränkungen - Empfang und Bearbeitung von Anfragen auf vertrauliche Kommunikation - Empfang von Datenschutzbeschwerden - Bereitstellung der Notice of Privacy Practices

Hinweis: Diese Rolle kann vom Privacy Officer oder einem Beauftragten ausgefüllt werden.

5.4 4. Unterstützende Rollen

5.4.1 4.1 HIPAA Compliance Manager

Name: [TODO: Name]
E-Mail: [TODO: E-Mail]
Telefon: [TODO: Telefon]

Verantwortlichkeiten: - Tägliche HIPAA-Compliance-Programmverwaltung - Richtlinien- und Verfahrenspflege - Schulungskoordination - Compliance-Überwachung und -Prüfung - Dokumentationsverwaltung - Lieferantenverwaltungsunterstützung - Compliance-Berichterstattung

5.4.2 4.2 IT-Sicherheitsmanager

Name: [TODO: Name]
E-Mail: [TODO: E-Mail]
Telefon: [TODO: Telefon]

Verantwortlichkeiten: - Implementierung technischer Schutzmaßnahmen - Zugriffskontrollverwaltung - Sicherheitsüberwachung und -protokollierung - Schwachstellenscanning und -behebung - Patch-Management - Verschlüsselungsimplementierung - Netzwerksicherheit - Incident Response (technisch)

5.5 5. RACI-Matrizen

5.5.1 5.1 Privacy Rule-Compliance

Aktivität	CEO	Privacy Officer	Security Officer	Abteilungsleiter	Recht
Datenschutzrichtlinien	A	R	C	C	C
Notice of Privacy Practices	A	R	I	I	C
Individuelle Zugriffsanfragen	I	A/R	I	C	C
Datenschutzbeschwerden	I	A/R	I	C	C
Datenschutzschulung	A	R	C	C	I
Datenschutzvorfälle	I	A/R	C	C	C
BAA-Verwaltung	A	R	C	C	R

5.5.2 5.2 Security Rule-Compliance

Aktivität	CEO	Privacy Officer	Security Officer	IT-Manager	Abteilungsleiter
Sicherheitsrichtlinien	A	C	R	C	C
Risikoanalyse	A	C	R	C	C
Zugriffskontrolle	I	C	A/R	R	C
Audit-Kontrollen	I	C	A/R	R	I
Sicherheitsvorfälle	I	C	A/R	R	C
Sicherheitsschulung	A	C	R	C	C
Schwachstellenmanagement	I	C	A	R	I

Legende: - **R** (Responsible): Führt die Arbeit aus - **A** (Accountable): Ultimative Verantwortung, genehmigt Arbeit (nur ein A pro Aktivität) - **C** (Consulted): Stellt Input bereit, bidirektionale Kommunikation - **I** (Informed): Wird informiert, unidirektionale Kommunikation

5.6 6. HIPAA Compliance Committee

5.6.1 6.1 Committee-Struktur

Committee-Name: HIPAA Compliance Committee

Vorsitz: {{ meta.roles.privacy_officer.name }} (Privacy Officer)

Mitglieder: - CEO oder Beauftragter - Privacy Officer - Security Officer - CIO oder IT-Direktor - Compliance Officer - Rechtsberater - Risikomanager - HR-Direktor - Klinischer Direktor (falls zutreffend) - Abteilungsvertreter

Sitzungshäufigkeit: [TODO: Monatlich/Vierteljährlich]

Quorum: [TODO: Mindestanzahl der Mitglieder]

5.6.2 6.2 Committee-Verantwortlichkeiten

- Aufsicht über HIPAA-Compliance-Programm
- Überprüfung und Genehmigung von Richtlinien und Verfahren
- Überprüfung von Risikobewertungen und Minderungsplänen
- Überprüfung von Datenschutz- und Sicherheitsvorfällen
- Überprüfung der Schulungseffektivität
- Budgetempfehlungen für Compliance-Aktivitäten
- Überprüfung regulatorischer Updates
- Überprüfung von Audit-Ergebnissen
- Kontinuierliche Verbesserungsinitiativen

5.7 7. Eskalationsverfahren

5.7.1 7.1 Datenschutzvorfall-Eskalation

Ebene 1: Datenschutzkoordinator (Abteilung)
Ebene 2: Privacy Officer
Ebene 3: CEO + Rechtsberater

Eskalationskriterien: - Vermuteter Verstoß gegen ungesicherte PHI - Unbefugter Zugriff auf PHI - Datenschutzbeschwerde von Einzelperson - OCR-Untersuchung - Medienanfrage

Reaktionszeit: - Ebene 1: Sofort - Ebene 2: Innerhalb 1 Stunde - Ebene 3: Innerhalb 4 Stunden

5.7.2 7.2 Sicherheitsvorfall-Eskalation

Ebene 1: IT-Help-Desk / Systemadministrator
Ebene 2: Security Officer
Ebene 3: CIO + CEO

Eskalationskriterien: - Vermuteter Sicherheitsverstoß - Malware-Infektion - Unbefugter Systemzugriff - Systemkompromittierung - Datenexfiltration - Ransomware

Reaktionszeit: - Ebene 1: Sofort - Ebene 2: Innerhalb 30 Minuten - Ebene 3: Innerhalb 1 Stunde

5.7.3 7.3 24/7-Kontaktinformationen

Sicherheits-Hotline: [TODO: Telefonnummer]
Datenschutz-Hotline: [TODO: Telefonnummer]
Außerhalb der Geschäftszeiten: [TODO: Bereitschaftsrotation oder Anrufbeantworter]

Notfallkontakte: | Rolle | Name | Mobil | E-Mail | |——|——|——-|——| | Privacy Officer | {{ meta.roles.privacy_officer.name }} | [TODO: Mobil] | {{ meta.roles.privacy_officer.email }} | | Security Officer | {{ meta.roles.security_officer.name }} | [TODO: Mobil] | {{ meta.roles.security_officer.email }} | | CEO | {{ meta.roles.ceo.name }} | [TODO: Mobil] | {{ meta.roles.ceo.email }} |

5.8 8. Schulung und Kompetenz

5.8.1 8.1 Rollenspezifische Schulung

Rolle	Erforderliche Schulung	Häufigkeit	Anbieter
Alle Belegschaft	HIPAA-Grundlagen	Jährlich	[TODO: LMS/Anbieter]
Privacy Officer	Privacy Rule-Vertiefung	Jährlich	[TODO: Extern]
Security Officer	Security Rule-Vertiefung	Jährlich	[TODO: Extern]
IT-Personal	Technische Schutzmaßnahmen	Jährlich	[TODO: Intern/Extern]
Klinisches Personal	PHI-Handhabung	Jährlich	[TODO: Intern]
Manager	Belegschaftsverwaltung	Jährlich	[TODO: Intern]

5.8.2 8.2 Kompetenzanforderungen

Privacy Officer: - Kenntnisse der HIPAA Privacy Rule - Verständnis des Gesundheitswesens - Untersuchungsfähigkeiten - Kommunikationsfähigkeiten - Erfahrung in Richtlinienentwicklung

Security Officer: - Kenntnisse der HIPAA Security Rule - Technische Sicherheitsexpertise - Risikobewertungsfähigkeiten - Incident-Response-Erfahrung - Kenntnisse der Sicherheitsarchitektur

5.9 9. Leistungsmetriken

5.9.1 9.1 Compliance-Metriken

Metrik	Ziel	Messung	Häufigkeit
Schulungsabschlussrate	100%	% geschulte Belegschaft	Vierteljährlich
Incident-Response-Zeit	< 1 Stunde	Zeit bis Eindämmung	Pro Vorfall
Zugriffsanfrage-Reaktionszeit	< 30 Tage	Tage bis Erfüllung	Pro Anfrage
Risikobewertungsabschluss	100%	Jährlicher Abschluss	Jährlich

Metrik	Ziel	Messung	Häufigkeit
Richtlinienüberprüfungsabschluss	100%	% überprüfte Richtlinien	Jährlich

---

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 6

HIPAA Compliance-Programm

Dokument-ID: HIPAA-0050
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

6.1 1. Zweck

Dieses Dokument beschreibt das HIPAA-Compliance-Programm für AdminSend GmbH, einschließlich Programmstruktur, Aktivitäten, Überwachung und kontinuierlicher Verbesserungsprozesse.

6.1.1 1.1 Zielsetzungen

- **Programmrahmen:** Umfassendes HIPAA-Compliance-Programm etablieren
- **Systematischer Ansatz:** Strukturierte Compliance-Aktivitäten definieren
- **Kontinuierliche Verbesserung:** Laufende Überwachung und Verbesserung implementieren
- **Verantwortlichkeit:** Klare Verantwortlichkeiten für Compliance-Aktivitäten zuweisen

6.1.2 1.2 Programmumfang

Abgedeckte HIPAA-Regeln: - Privacy Rule (45 CFR Part 164, Subpart E) - Security Rule (45 CFR Part 164, Subpart C) - Breach Notification Rule (45 CFR Part 164, Subpart D) - Enforcement Rule (45 CFR Part 160, Subparts C, D, E)

6.2 2. Compliance-Programmstruktur

6.2.1 2.1 Programmkomponenten

1. Governance und Führung - Geschäftsführungsaufsicht - Privacy und Security Officers - HIPAA Compliance Committee - Ressourcenzuweisung

2. Richtlinien und Verfahren - Datenschutzrichtlinien - Sicherheitsrichtlinien - Breach Notification-Verfahren - Belegschaftsrichtlinien

3. Risikomanagement - Risikoanalyse - Risikomanagement - Risikominderung - Laufende Risikobewertung

4. Schulung und Sensibilisierung - Erstschulung - Jährliche Schulung - Rollenspezifische Schulung - Sensibilisierungskampagnen

5. Überwachung und Prüfung - Compliance-Überwachung - Interne Audits - Externe Bewertungen - Korrekturmaßnahmen

6. Incident Management - Datenschutzvorfälle - Sicherheitsvorfälle - Verstoßbewertung - Verstoßmeldung

7. Business Associate-Verwaltung - BA-Identifikation - BAA-Ausführung - BA-Überwachung - BA-Beendigung

8. Individuelle Rechte - Zugriffsanfragen - Änderungsanfragen - Rechenschaftspflicht über Offenlegungen - Einschränkungsanfragen - Vertrauliche Kommunikation

9. Dokumentation und Aufzeichnungen - Richtliniendokumentation - Schulungsunterlagen - Vorfallsaufzeichnungen - Audit-Aufzeichnungen

10. Kontinuierliche Verbesserung - Programmbewertung - Lessons Learned - Best Practices - Regulatorische Updates

6.3 3. Compliance-Programmaktivitäten

6.3.1 3.1 Jährliche Aktivitäten

Aktivität	Verantwortlich	Zeitplan	Ergebnis
Risikoanalyse	Security Officer	Q1	Risikoanalysebericht
Richtlinienüberprüfung	Privacy Officer	Q2	Aktualisierte Richtlinien
Internes Audit	Compliance Manager	Q3	Audit-Bericht
Schulungsprogrammüberprüfung	Privacy Officer	Q4	Schulungsbewertung
Programmbewertung	Compliance Officer	Q4	Jahresbericht
Managementbewertung	CEO	Q4	Managementbewertungsprotokoll

6.3.2 3.2 Vierteljährliche Aktivitäten

Aktivität	Verantwortlich	Ergebnis
Compliance Committee-Sitzung	Privacy Officer	Sitzungsprotokoll
Metrikenüberprüfung	Compliance Manager	Metriken-Dashboard
BA-Compliance-Überprüfung	Privacy Officer	BA-Statusbericht
Vorfallstrendanalyse	Security Officer	Vorfallsbericht
Schulungsabschlussüberprüfung	Schulungskoordinator	Schulungsbericht

6.3.3 3.3 Monatliche Aktivitäten

Aktivität	Verantwortlich	Ergebnis
Zugriffsüberprüfung	Security Officer	Zugriffsüberprüfungsbericht
Audit-Log-Überprüfung	IT-Sicherheit	Log-Überprüfungszusammenfassung
Vorfallsüberprüfung	Privacy/Security Officers	Vorfallszusammenfassung
Schulungsverfolgung	Schulungskoordinator	Schulungsstatus
Richtlinienaktualisierungen	Compliance Manager	Änderungsprotokoll

6.3.4 3.4 Laufende Aktivitäten

Aktivität	Verantwortlich	Häufigkeit
Individuelle Rechtsanfragen	Privacy Officer	Bei Eingang
Datenschutzbeschwerden	Privacy Officer	Bei Eingang
Sicherheitsvorfälle	Security Officer	Bei Erkennung
Datenschutzvorfälle	Privacy Officer	Bei Erkennung
Verstoßbewertung	Privacy/Security Officers	Nach Bedarf
Belegschafts-Onboarding	HR + Privacy Officer	Nach Bedarf
Belegschafts-Offboarding	HR + Security Officer	Nach Bedarf

6.4 4. Richtlinien und Verfahren

6.4.1 4.1 Richtlinienrahmen

Richtlinienhierarchie: 1. **HIPAA-Compliance-Richtlinie** (Dieses Dokument) 2. **Datenschutzrichtlinien** (HIPAA-0500-Serie) 3. **Sicherheitsrichtlinien** (HIPAA-0100-0400-Serie) 4. **Betriebsverfahren** (Abteilungsspezifisch) 5. **Arbeitsanweisungen** (Aufgabenspezifisch)

6.4.2 4.2 Richtlinienentwicklungsprozess

Prozessschritte: 1. Bedarf für Richtlinie identifizieren 2. Richtlinie entwerfen (Privacy/Security Officer) 3. Stakeholder-Überprüfung 4. Rechtliche Überprüfung 5. Compliance Committee-Genehmigung 6. Geschäftsführungsgenehmigung 7. Kommunikation und Schulung 8. Implementierung 9. Überwachung und Durchsetzung

6.4.3 4.3 Richtlinienüberprüfung und -aktualisierung

Überprüfungsplan: - **Jährliche Überprüfung:** Alle Richtlinien jährlich überprüft - **Ausgelöste Überprüfung:** Bei Regulierungsänderungen, Vorfällen oder Betriebsänderungen - **Versionskontrolle:** Alle Richtlinien versionskontrolliert

Überprüfungsprozess: 1. Privacy/Security Officer initiiert Überprüfung 2. Aktuelle Richtlinieneffektivität bewerten 3. Erforderliche Änderungen identifizieren 4. Richtlinie aktualisieren 5. Genehmigungsprozess wiederholen 6. Änderungen kommunizieren 7. Schulungsmaterialien aktualisieren

6.5 5. Schulungsprogramm

6.5.1 5.1 Schulungsanforderungen

HIPAA-Schulung erforderlich für: - Alle Belegschaftsmitglieder (Mitarbeiter, Freiwillige, Auszubildende, Auftragnehmer) - Business Associates (empfohlen) - Neueinstellungen (innerhalb 30 Tage) - Jährliche Auffrischungsschulung - Bei wesentlichen Richtlinienänderungen

Schulungsthemen: - HIPAA-Überblick und Anwendbarkeit - Privacy Rule-Anforderungen - Security Rule-Anforderungen - Breach Notification Rule - Individuelle Rechte - Zulässige Nutzungen und Offenlegungen - Minimum Necessary-Standard - Autorisierungsanforderungen - Sicherheitsschutzmaßnahmen - Vorfallsmeldung - Sanktionen bei Verstößen - Organisationsspezifische Richtlinien

6.5.2 5.2 Schulungsdurchführung

Schulungsmethoden: - Online-Lernmanagementsystem (LMS) - Präsenzsitzungen - Abteilungsbesprechungen - Neueinstellungsorientierung - Rollenspezifische Schulung - Just-in-Time-Schulung

Schulungsmaterialien: - Schulungsmodule - Kurzreferenzleitfäden - Poster und Erinnerungen - E-Mail-Kommunikation - Intranet-Ressourcen

6.5.3 5.3 Schulungsverfolgung

Erforderliche Dokumentation: - Schulungsteilnahmeaufzeichnungen - Schulungsabschlusszertifikate - Testergebnisse (falls zutreffend) - Bereitgestellte Schulungsmaterialien - Schulungsdaten und -dauer

Aufbewahrung: [TODO: 6 Jahre]

Schulungsdatenbank: [TODO: LMS oder Verfolgungssystem]

6.6 6. Überwachung und Prüfung

6.6.1 6.1 Compliance-Überwachung

Überwachungsaktivitäten: - Zugriffslog-Überprüfungen - Audit-Trail-Überprüfungen - Richtlinien-Compliance-Prüfungen - Sicherheitskontrolltests - Datenschutzpraxisbeobachtungen - Beschwerdeuntersuchungen - Vorfallsüberprüfungen

Überwachungsplan: | Aktivität | Häufigkeit | Verantwortlich | |———-|———-|————| | Zugriffslog-Überprüfung | Monatlich | Security Officer | | Audit-Trail-Überprüfung | Monatlich |

IT-Sicherheit | | Richtlinien-Compliance-Stichproben | Vierteljährlich | Compliance Manager | | Sicherheitskontrolltests | Vierteljährlich | Security Officer | | Datenschutzpraxis-Audits | Halbjährlich | Privacy Officer |

6.6.2 6.2 Internes Auditprogramm

Audit-Umfang: - Privacy Rule-Compliance - Security Rule-Compliance - Breach Notification-Compliance - Richtlinieneinhaltung - Schulungseffektivität - Business Associate-Verwaltung - Individuelle Rechtsbearbeitung - Dokumentation und Aufzeichnungen

Audit-Häufigkeit: Jährlich (Minimum)

Audit-Prozess: 1. Audit-Plan entwickeln 2. Auditees benachrichtigen 3. Audit durchführen (Interviews, Dokumentenprüfung, Tests) 4. Ergebnisse dokumentieren 5. Ergebnisse berichten 6. Korrekturmaßnahmenplan entwickeln 7. Korrekturen implementieren 8. Korrekturen verifizieren 9. Audit abschließen

Audit-Dokumentation: - Audit-Plan - Audit-Checkliste - Ergebnisse und Beobachtungen - Korrekturmaßnahmenplan - Follow-up-Verifizierung

6.7 7. Incident Management

6.7.1 7.1 Vorfallstypen

Datenschutzvorfälle: - Unbefugter Zugriff auf PHI - Unbefugte Offenlegung von PHI - Unsachgemäße Nutzung von PHI - Verlust oder Diebstahl von PHI - Datenschutzbeschwerden

Sicherheitsvorfälle: - Unbefugter Systemzugriff - Malware-Infektion - Phishing-Angriffe - Verlorene oder gestohlene Geräte - Systemschwachstellen - Denial of Service

6.7.2 7.2 Incident-Response-Prozess

Prozessschritte: 1. **Erkennung und Meldung** - Vorfall identifiziert - An Privacy/Security Officer gemeldet - Erstbewertung

2. **Eindämmung**
   - Laufenden Vorfall stoppen
   - Weiteren Schaden verhindern
   - Beweise sichern
3. **Untersuchung**
   - Umfang und Auswirkung bestimmen
   - Grundursache identifizieren
   - Ergebnisse dokumentieren
4. **Verstoßbewertung**
   - Verstoßrisikobewertung anwenden
   - Bestimmen, ob Verstoß aufgetreten ist
   - Meldepflichten bewerten
5. **Benachrichtigung** (bei Verstoß)
   - Einzelpersonen benachrichtigen
   - HHS benachrichtigen
   - Medien benachrichtigen (bei 500+ Personen)

6. **Behebung**
   - Korrekturmaßnahmen implementieren
   - Schwachstellen mindern
   - Kontrollen aktualisieren
7. **Dokumentation**
   - Vorfallsbericht
   - Untersuchungsergebnisse
   - Ergriffene Maßnahmen
   - Lessons Learned
8. **Follow-up**
   - Auf Wiederholung überwachen
   - Wirksamkeit der Korrekturen verifizieren
   - Richtlinien/Verfahren aktualisieren

6.8 8. Metriken und Berichterstattung

6.8.1 8.1 Key Performance Indicators (KPIs)

KPI	Ziel	Messung	Häufigkeit
Schulungsabschlussrate	100%	% geschulte Belegschaft	Vierteljährlich
Incident-Response-Zeit	< 1 Stunde	Zeit bis Eindämmung	Pro Vorfall
Zugriffsanfrage-Reaktionszeit	< 30 Tage	Tage bis Erfüllung	Pro Anfrage
Risikobewertungsabschluss	100%	Jährlicher Abschluss	Jährlich
Richtlinienüberprüfung	100%	% überprüfte Richtlinien	Jährlich
Audit-Ergebnisabschluss	< 90 Tage	Tage bis Abschluss	Pro Ergebnis
BA-BAA-Abdeckung	100%	% BAs mit aktuellem BAA	Vierteljährlich

6.8.2 8.2 Berichtsstruktur

Monatliche Berichte: - Vorfallszusammenfassung - Schulungsstatus - Bearbeitete Zugriffsanfragen - Metriken-Dashboard

Vierteljährliche Berichte: - Compliance-Metriken - Audit-Status - Risiko-Updates - BA-Compliance

Jährliche Berichte: - Umfassende Programmüberprüfung - Risikoanalyseergebnisse - Schulungseffektivität - Audit-Ergebnisse - Verbesserungsinitiativen - Budget und Ressourcen

Berichtsempfänger: - CEO - Compliance Committee - Vorstand (jährlich) - Abteilungsleiter (relevante Abschnitte)

6.9 9. Kontinuierliche Verbesserung

6.9.1 9.1 Verbesserungsprozess

Verbesserungsquellen: - Lessons Learned aus Vorfällen - Audit-Ergebnisse - Regulatorische Änderungen - Branchen-Best-Practices - Technologiefortschritte - Belegschafts-Feedback

Verbesserungszyklus: 1. Verbesserungsmöglichkeit identifizieren 2. Aktuellen Zustand bewerten 3. Gewünschten Zustand definieren 4. Verbesserungsplan entwickeln 5. Änderungen implementieren 6. Wirksamkeit überwachen 7. Verbesserungen standardisieren 8. Dokumentieren und kommunizieren

6.9.2 9.2 Regulatorische Überwachung

Überwachungsaktivitäten: - HHS-Website-Überwachung - Federal Register-Überwachung - Branchenverbands-Updates - Rechtsberater-Updates - Compliance-Newsletter - Webinare und Konferenzen

Regulatorischer Änderungsprozess: 1. Regulatorische Änderung identifizieren 2. Auswirkung auf Organisation bewerten 3. Compliance-Plan entwickeln 4. Richtlinien und Verfahren aktualisieren 5. Belegschaft schulen 6. Änderungen implementieren 7. Compliance überwachen

6.10 10. Programmbewertung

6.10.1 10.1 Jährliche Programmbewertung

Bewertungskomponenten: - Programmeffektivitätsüberprüfung - Zielerreichungsbewertung - Ressourcenangemessenheitsüberprüfung - Stakeholder-Feedback - Benchmarking gegen Branche - Gap-Analyse

Bewertungsprozess: 1. Daten sammeln (Metriken, Audit-Ergebnisse, Vorfälle) 2. Trends analysieren 3. Stärken und Schwächen identifizieren 4. Empfehlungen entwickeln 5. Compliance Committee präsentieren 6. Geschäftsführung präsentieren 7. Verbesserungsplan entwickeln 8. Ressourcen zuweisen 9. Verbesserungen implementieren

---

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 7

Sicherheitsmanagement-Prozess

Dokument-ID: HIPAA-0100
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

7.1 1. Zweck

Dieses Dokument beschreibt den Sicherheitsmanagement-Prozess für AdminSend GmbH, einschließlich Risikoanalyse, Risikomanagement, Sanktionsrichtlinie und Überprüfung der Informationssystemaktivitäten gemäß HIPAA Security Rule §164.308(a)(1).

7.1.1 1.1 HIPAA-Anforderung

Standard: §164.308(a)(1) - Sicherheitsmanagement-Prozess (Erforderlich)

Implementierungsspezifikationen: - §164.308(a)(1)(ii)(A) - Risikoanalyse (Erforderlich) - §164.308(a)(1)(ii)(B) - Risikomanagement (Erforderlich) - §164.308(a)(1)(ii)(C) - Sanktionsrichtlinie (Erforderlich) - §164.308(a)(1)(ii)(D) - Überprüfung der Informationssystemaktivitäten (Erforderlich)

7.2 2. Risikoanalyse

7.2.1 2.1 Risikoanalyseprozess

Anforderung: Durchführung einer genauen und gründlichen Bewertung der potenziellen Risiken und Schwachstellen für die Vertraulichkeit, Integrität und Verfügbarkeit von ePHI.

Prozessschritte: 1. **Geltungsbereichsdefinition** - Alle ePHI innerhalb der Organisation identifizieren - Systeme, Anwendungen und Standorte definieren - Belegschaft mit ePHI-Zugriff identifizieren

2. **Datenerfassung**
   - IT-Assets inventarisieren
   - Datenflüsse dokumentieren
   - Aktuelle Sicherheitsmaßnahmen identifizieren
   - Richtlinien und Verfahren überprüfen
3. **Bedrohungsidentifikation**
   - Natürliche Bedrohungen (Feuer, Überschwemmung, Erdbeben)
   - Menschliche Bedrohungen (unbefugter Zugriff, böswilliger Insider, Social Engineering)
   - Umweltbedrohungen (Stromausfall, Hardwareausfall)
4. **Schwachstellenbewertung**
   - Technische Schwachstellen
   - Physische Schwachstellen
   - Administrative Schwachstellen
5. **Risikobestimmung**
   - Wahrscheinlichkeitsbewertung
   - Auswirkungsbewertung
   - Risikolevelberechnung
6. **Dokumentation**
   - Risikoanalysebericht
   - Risikoregister
   - Empfehlungen

Häufigkeit: Jährlich (Minimum) oder bei wesentlichen Änderungen

Verantwortlich: {{ meta.roles.security_officer.name }} (Security Officer)

7.2.2 2.2 Risikoanalysemethodik

Risikobewertungsformel:

```
Risiko = Wahrscheinlichkeit × Auswirkung
```

Wahrscheinlichkeitsskala: - **Hoch (3):** Sehr wahrscheinlich (> 50% Wahrscheinlichkeit) - **Mittel (2):** Möglich (10-50% Wahrscheinlichkeit) - **Niedrig (1):** Unwahrscheinlich (< 10% Wahrscheinlichkeit)

Auswirkungsskala: - **Hoch (3):** Schwerwiegende Auswirkung auf Vertraulichkeit, Integrität oder Verfügbarkeit - **Mittel (2):** Moderate Auswirkung - **Niedrig (1):** Minimale Auswirkung

Risikolevel: - **Kritisch (7-9):** Sofortige Maßnahme erforderlich - **Hoch (5-6):** Maßnahme innerhalb 30 Tage erforderlich - **Mittel (3-4):** Maßnahme innerhalb 90 Tage erforderlich - **Niedrig (1-2):** Überwachen und überprüfen

7.2.3 2.3 Risikoregister

Risiko-ID	Bedrohung	Schwachstelle	Wahrscheinlichkeit	Auswirkung	Risikolevel	Minderung	Verantwortlich	Status
[TODO: R-001]	[TODO: Unbefugter Zugriff]	[TODO: Schwache Passwörter]	[TODO: Hoch]	[TODO: Hoch]	[TODO: Kritisch]	[TODO: MFA implementieren]	[TODO: Security Officer]	[TODO: Offen]
[TODO: R-002]	[TODO: Malware]	[TODO: Kein Endpoint-Schutz]	[TODO: Mittel]	[TODO: Hoch]	[TODO: Hoch]	[TODO: EDR bereitstellen]	[TODO: IT-Manager]	[TODO: In Bearbeitung]

7.3 3. Risikomanagement

7.3.1 3.1 Risikomanagementprozess

Anforderung: Sicherheitsmaßnahmen implementieren, die ausreichen, um Risiken und Schwachstellen auf ein angemessenes und geeignetes Niveau zu reduzieren.

Risikobehandlungsoptionen: 1. **Mindern:** Kontrollen implementieren, um Risiko zu reduzieren 2. **Akzeptieren:** Risiko akzeptieren, wenn innerhalb akzeptablen Niveaus 3. **Übertragen:** Risiko übertragen (z.B. Versicherung, Outsourcing) 4. **Vermeiden:** Aktivität eliminieren, die das Risiko verursacht

7.3.2 3.2 Risikominderungsplan

Risiko-ID	Minderungsstrategie	Zu implementierende Kontrollen	Zeitplan	Budget	Verantwortlich	Status
[TODO: R-001]	Mindern	Multi-Faktor-Authentifizierung	[TODO: 30 Tage]	[TODO: $X]	[TODO: Security Officer]	[TODO: Geplant]
[TODO: R-002]	Mindern	Endpoint Detection and Response	[TODO: 60 Tage]	[TODO: $X]	[TODO: IT-Manager]	[TODO: In Bearbeitung]

7.3.3 3.3 Restrisiko

Restrisikobewertung: Nach Implementierung von Kontrollen Risikolevel neu bewerten, um Restrisiko zu bestimmen.

Risiko-ID	Anfängliches Risikolevel	Implementierte Kontrollen	Restrisiko-Level	Akzeptanz
[TODO: R-001]	Kritisch (9)	MFA, Passwortrichtlinie	Mittel (4)	Akzeptiert

Risiko-ID	Anfängliches Risikolevel	Implementierte Kontrollen	Restrisiko-Level	Akzeptanz
[TODO: R-002]	Hoch (6)	EDR, Antivirus	Niedrig (2)	Akzeptiert

Risikoakzeptanz: - Restrisiken müssen formal vom Management akzeptiert werden - Akzeptanz mit Begründung dokumentiert - Regelmäßige Überprüfung akzeptierter Risiken

7.4 4. Sanktionsrichtlinie

7.4.1 4.1 Richtlinienerklärung

Anforderung: Angemessene Sanktionen gegen Belegschaftsmitglieder anwenden, die Sicherheitsrichtlinien und -verfahren nicht einhalten.

Richtlinie: AdminSend GmbH wird angemessene Sanktionen gegen Belegschaftsmitglieder anwenden, die HIPAA-Sicherheitsrichtlinien und -verfahren verletzen. Sanktionen werden konsistent und fair angewendet, entsprechend der Schwere des Verstoßes.

7.4.2 4.2 Verstöße und Sanktionen

Verstößtypen:

Stufe 1 - Geringfügige Verstöße: - Unbeabsichtigter, isolierter Richtlinienverstoß - Kein Schaden für ePHI - Beispiele: Arbeitsstation unverschlossen gelassen, Passwort aufgeschrieben

Sanktionen: - Mündliche Verwarnung - Obligatorische Nachschulung - Dokumentation in Personalakte

Stufe 2 - Moderate Verstöße: - Wiederholte geringfügige Verstöße - Fahrlässiges Verhalten - Beispiele: Wiederholtes Passwort-Sharing, Zugriff auf unnötige ePHI

Sanktionen: - Schriftliche Verwarnung - Obligatorische Nachschulung - Aussetzung des Systemzugriffs (vorübergehend) - Leistungsverbesserungsplan

Stufe 3 - Schwerwiegende Verstöße: - Vorsätzlicher Richtlinienverstoß - Potenzieller Schaden für ePHI - Beispiele: Unbefugte Offenlegung, Zugriff auf ePHI ohne Autorisierung

Sanktionen: - Unbezahlte Suspendierung - Kündigung des Arbeitsverhältnisses - Widerruf des Systemzugriffs - Rechtliche Schritte (falls zutreffend)

Stufe 4 - Kritische Verstöße: - Vorsätzlicher Verstoß gegen ePHI - Kriminelle Aktivität - Beispiele: Diebstahl von ePHI, Verkauf von ePHI, böswillige Zerstörung

Sanktionen: - Sofortige Kündigung - Strafrechtliche Verfolgung - Meldung an Strafverfolgungsbehörden - Meldung an HHS OCR

7.4.3 4.3 Sanktionsprozess

Prozessschritte: 1. **Vorfallsentdeckung:** Verstoß identifiziert 2. **Untersuchung:** Security Officer untersucht 3. **Bestimmung:** Verstoßstufe bestimmen 4. **Konsultation:** Mit HR und Rechtsabteilung konsultieren 5. **Sanktionsentscheidung:** Management entscheidet über

angemessene Sanktion 6. **Implementierung:** Sanktion anwenden 7. **Dokumentation:** In Personalakte und Vorfallsprotokoll dokumentieren 8. **Follow-up:** Auf Wiederholung überwachen

Ordnungsgemäßes Verfahren: - Belegschaftsmitglied über angeblichen Verstoß benachrichtigt - Gelegenheit zur Stellungnahme - Faire und unparteiische Untersuchung - Konsistente Anwendung von Sanktionen

7.4.4 4.4 Sanktionsprotokoll

Datum	Mitarbeiter-ID	Verstoß	Stufe	Angewandte Sanktion	Angewendet durch	Status
[TODO: Datum]	[TODO: EMP-XXX]	[TODO: Beschreibung]	[TODO: Stufe]	[TODO: Sanktion]	[TODO: Manager]	[TODO: Abgeschlossen]

Aufbewahrung: [TODO: 6 Jahre]

7.5 5. Überprüfung der Informationssystemaktivitäten

7.5.1 5.1 Überprüfungsanforderungen

Anforderung: Verfahren implementieren, um regelmäßig Aufzeichnungen der Informationssystemaktivitäten zu überprüfen, wie Audit-Logs, Zugriffsberichte und Sicherheitsvorfall-Tracking-Berichte.

Zweck: - Sicherheitsvorfälle erkennen - Richtlinienverstöße identifizieren - Systemleistung überwachen - Untersuchungen unterstützen - Compliance nachweisen

7.5.2 5.2 Überprüfungsaktivitäten

Tägliche Überprüfungen: - Fehlgeschlagene Anmeldeversuche - Kritische Systemwarnungen - Sicherheitstool-Warnungen (IDS/IPS, Antivirus) - Privilegierte Kontoaktivität

Wöchentliche Überprüfungen: - Zugriffslogs für sensible Systeme - Benutzerkonto-Änderungen - Firewall-Logs - VPN-Zugriffslogs

Monatliche Überprüfungen: - Umfassende Audit-Log-Überprüfung - Zugriffsrechte-Überprüfung - Sicherheitsvorfall-Trends - Richtlinien-Compliance-Prüfungen

Vierteljährliche Überprüfungen: - Benutzerzugriffs-Rezertifizierung - Privilegierte Konto-Überprüfung - Sicherheitskontroll-Effektivität - Risikobewertungs-Updates

7.5.3 5.3 Audit-Log-Anforderungen

Systeme, die Audit-Logging erfordern: - Alle Systeme mit ePHI - Authentifizierungssysteme - Netzwerkgeräte (Firewalls, Router) - Datenbanksysteme - Anwendungsserver - E-Mail-Systeme

Zu protokollierende Ereignisse: - Benutzer-Login/Logout - Zugriff auf ePHI - Änderungen an ePHI - Benutzerkonto-Änderungen - Berechtigungsänderungen - Systemkonfigurationsänderungen - Sicherheitsereignisse (fehlgeschlagene Logins, Malware-Erkennung)

Log-Aufbewahrung: [TODO: 6 Jahre Minimum]

7.5.4 5.4 Überprüfungsdokumentation

Überprüfungsprotokoll: | Überprüfungsdatum | Prüfer | Überprüfte Systeme | Ergebnisse | Ergriffene Maßnahmen | Follow-up erforderlich | |———————-|———|———————-|————|———————-|———————-| | [TODO: Datum] | [TODO: Name] | [TODO: Systeme] | [TODO: Ergebnisse] | [TODO: Maßnahmen] | [TODO: Ja/Nein] |

Ergebnisse und Maßnahmen: - Alle Ergebnisse dokumentieren - Korrekturmaßnahmen zuweisen - Bis zum Abschluss verfolgen - Wesentliche Ergebnisse eskalieren

7.6 6. Dokumentation und Aufzeichnungen

7.6.1 6.1 Erforderliche Dokumentation

- Risikoanalyseberichte
- Risikoregister
- Risikomanagementpläne
- Sanktionsrichtlinie
- Sanktionsprotokoll
- Audit-Log-Überprüfungsverfahren
- Überprüfungsprotokolle und Ergebnisse
- Korrekturmaßnahmenpläne

7.6.2 6.2 Aufbewahrung

Aufbewahrungsfrist: [TODO: 6 Jahre ab Erstellung oder letztem Gültigkeitsdatum]

Speicherort: [TODO: Dokumentenmanagementsystem-Standort]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 8

Mitarbeitersicherheit

Dokument-ID: HIPAA-0110
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

8.1 1. Zweck

Dieses Dokument beschreibt die Verfahren zur Mitarbeitersicherheit für AdminSend GmbH, um sicherzustellen, dass alle Mitarbeiter angemessenen Zugang zu ePHI haben und unbefugter Zugriff verhindert wird.

8.1.1 1.1 HIPAA-Anforderung

Standard: §164.308(a)(3) - Workforce Security (Erforderlich)

Implementierungsspezifikationen: - §164.308(a)(3)(ii)(A) - Autorisierung und/oder Überwachung (Adressierbar) - §164.308(a)(3)(ii)(B) - Verfahren zur Mitarbeiterfreigabe (Adressierbar) - §164.308(a)(3)(ii)(C) - Kündigungsverfahren (Adressierbar)

8.2 2. Autorisierung und Überwachung

8.2.1 2.1 Zugriffsautorisierung

Prinzip: Der Zugriff auf ePHI wird basierend auf Rolle, Jobfunktion und dem Prinzip der minimalen Notwendigkeit gewährt.

Autorisierungsprozess: 1. **Jobanalyse:** Ermittlung der ePHI-Zugriffsanforderungen für die Rolle 2. **Zugriffsanfrage:** Manager reicht Zugriffsanfrage ein 3. **Begründung:** Dokumentation

des geschäftlichen Bedarfs 4. **Genehmigung:** Privacy Officer und/oder Security Officer genehmigen 5. **Bereitstellung:** IT stellt Zugriff bereit 6. **Dokumentation:** Zugriff wird protokolliert 7. **Bestätigung:** Mitarbeiter bestätigt Verantwortlichkeiten

Autorisierungskriterien: - Jobrolle erfordert ePHI-Zugriff - Nur minimal notwendiger Zugriff - Angemessene Schulung abgeschlossen - Hintergrundprüfung abgeschlossen (falls erforderlich) - Vertraulichkeitsvereinbarung unterzeichnet

8.2.2 2.2 Überwachungsanforderungen

Überwachter Zugriff: Mitarbeiter mit begrenzter Schulung oder temporärem Status benötigen möglicherweise Überwachung beim Zugriff auf ePHI.

Überwachungsstufen: | Mitarbeitertyp | Überwachung erforderlich | Vorgesetzter | Dauer | |———-|———————-|———–|——-| | Neue Mitarbeiter (< 90 Tage) | Ja | Direkter Vorgesetzter | Bis Schulung abgeschlossen | | Zeitarbeitskräfte | Ja | Zugewiesener Vorgesetzter | Dauer der Beauftragung | | Praktikanten/Studenten | Ja | Betreuer/Ausbilder | Dauer des Programms | | Auftragnehmer (kurzfristig) | Ja | Projektmanager | Dauer des Vertrags |

Verantwortlichkeiten des Vorgesetzten: - Überwachung des ePHI-Zugriffs des Mitarbeiters - Sicherstellung der Einhaltung von Richtlinien - Bereitstellung von Anleitung und Schulung - Meldung von Verstößen - Dokumentation der Überwachungsaktivitäten

8.3 3. Verfahren zur Mitarbeiterfreigabe

8.3.1 3.1 Voreinstellungsüberprüfung

Anforderungen an Hintergrundprüfungen:

Alle Mitarbeiter mit ePHI-Zugriff: - Identitätsüberprüfung - Überprüfung der Beschäftigungshistorie (7 Jahre) - Überprüfung der Ausbildung - Überprüfung der beruflichen Lizenz (falls zutreffend)

Mitarbeiter mit erhöhtem Zugriff: - Kriminelle Hintergrundprüfung - Bonitätsprüfung (für Finanzrollen) - Referenzprüfungen (mindestens 3)

Hintergrundprüfungsprozess: 1. **Bedingtes Angebot:** Angebot abhängig von Hintergrundprüfung 2. **Autorisierung:** Kandidat autorisiert Hintergrundprüfung 3. **Überprüfung:** Drittanbieter führt Prüfung durch 4. **Prüfung:** HR prüft Ergebnisse 5. **Entscheidung:** Einstellungs-/Nicht-Einstellungsentscheidung 6. **Dokumentation:** Ergebnisse dokumentiert und gesichert 7. **Nachteilige Maßnahme:** FCRA-Anforderungen befolgen, falls nachteilige Maßnahme ergriffen wird

Hintergrundprüfungsanbieter: [TODO: Anbietername]

8.3.2 3.2 Freigabestufen

Freigabestufe	Anforderungen	Rollen	ePHI-Zugriff
Stufe 1 - Basis	Identitätsüberprüfung, Beschäftigungshistorie	Verwaltungspersonal	Begrenzter ePHI

Freigabestufe	Anforderungen	Rollen	ePHI-Zugriff
Stufe 2 - Standard	Stufe 1 + Ausbildungsüberprüfung	Klinisches Personal	Vollständiger ePHI für Patientenversorgung
Stufe 3 - Erhöht	Stufe 2 + kriminelle Hintergrundprüfung	IT-Personal, Abrechnung	Systemebenen-ePHI-Zugriff
Stufe 4 - Führungsebene	Stufe 3 + Bonitätsprüfung, Referenzen	Führungskräfte, Compliance	Alle ePHI

8.3.3 3.3 Laufende Freigabe

Periodische Nachprüfung: - **Häufigkeit:** [TODO: Alle 3-5 Jahre oder wie für Rolle erforderlich] - **Umfang:** Kriminelle Hintergrundprüfung, Lizenzüberprüfung - **Auslösende Ereignisse:** Beförderung, Rollenwechsel, Sicherheitsvorfall

Kontinuierliche Überwachung: - Status der beruflichen Lizenz - Sanktionen oder Disziplinarmaßnahmen - Strafrechtliche Verurteilungen (falls gesetzlich zulässig)

8.4 4. Kündigungsverfahren

8.4.1 4.1 Kündigungsprozess

Kündigungsarten: - Freiwillige Kündigung - Unfreiwillige Kündigung - Ruhestand - Ende des Vertrags/temporäre Beauftragung - Tod

Kündigungs-Checkliste:

Sofortige Maßnahmen (Tag der Kündigung): - [ ] Deaktivierung aller Systemzugriffe (innerhalb 1 Stunde nach Benachrichtigung) - [ ] Deaktivierung des E-Mail-Kontos - [ ] Deaktivierung des VPN-Zugriffs - [ ] Deaktivierung des physischen Zugriffs (Ausweis, Schlüssel) - [ ] Einsammeln von Firmengeräten (Laptop, Telefon, Tablet) - [ ] Einsammeln von Zugangsausweisen und Schlüsseln - [ ] Änderung gemeinsam genutzter Passwörter/Codes, die dem Mitarbeiter bekannt sind - [ ] Benachrichtigung von IT, Security und Facilities

Innerhalb von 24 Stunden: - [ ] Überprüfung und Archivierung der Dateien des Mitarbeiters - [ ] Weiterleitung von E-Mails an Manager (falls angemessen) - [ ] Entfernung aus Verteilerlisten - [ ] Aktualisierung von Organigrammen - [ ] Benachrichtigung relevanter Abteilungen - [ ] Dokumentation der Kündigung im HR-System

Innerhalb von 1 Woche: - [ ] Durchführung eines Austrittsgespräches - [ ] Erinnerung an Vertraulichkeitsverpflichtungen - [ ] Einsammeln der unterzeichneten Bestätigung der Verpflichtungen - [ ] Abschlusszahlung - [ ] COBRA-Benachrichtigung (falls zutreffend) - [ ] Überprüfung der Rückgabe von Eigentum

8.4.2 4.2 Zugriffskündigung

Systemzugriffskündigung: | System | Kündigungsmethode | Verantwortlich | Überprüfung | |——–|——————-|——————-|——————-| | Active Directory | Konto deaktiviert | IT | Automatisierter Bericht | | EHR-System | Benutzer deaktiviert | IT | Manuelle Überprüfung | | E-Mail | Postfach

deaktiviert | IT | Automatisierter Bericht | | VPN | Zertifikat widerrufen | IT | Manuelle Überprüfung | | Physischer Zugang | Ausweis deaktiviert | Facilities | Zugriffsprotokollprüfung |

Kündigungsüberprüfung: - IT erstellt Kündigungsbericht - Security Officer prüft Bericht - Ausnahmen werden untersucht und behoben - Dokumentation wird aufbewahrt

8.4.3 4.3 Wissenstransfer

Wissenstransferprozess: 1. **Identifikation:** Identifikation kritischen Wissens und Verantwortlichkeiten 2. **Dokumentation:** Dokumentation von Prozessen und Verfahren 3. **Schulung:** Schulung von Ersatz oder Teammitgliedern 4. **Übergang:** Schrittweiser Übergang von Verantwortlichkeiten (falls möglich) 5. **Überprüfung:** Überprüfung, dass Wissenstransfer abgeschlossen ist

Kritische Wissensbereiche: - Systemzugriff und Passwörter - Laufende Projekte - Wichtige Kontakte - Ausstehende Probleme - Dokumentationsspeicherorte

8.4.4 4.4 Überwachung nach Kündigung

Überwachungsaktivitäten: - Überprüfung von Audit-Protokollen für gekündigte Mitarbeiterkonten - Überwachung auf unbefugte Zugriffsversuche - Überprüfung auf Datenexfiltration - Überwachung auf Richtlinienverstöße vor Kündigung

Überwachungszeitraum: [TODO: 90 Tage nach Kündigung]

8.5 5. Rollenbasierte Zugriffskontrolle (RBAC)

8.5.1 5.1 Rollendefinitionen

Rollen-ID	Rollenname	Abteilung	ePHI-Zugriffsstufe	Systeme	Genehmigung erforderlich
[TODO: ROLE-001]	Arzt	Klinisch	Vollständige Patientenversorgung	EHR, Labor, Bildgebung	Ärztlicher Direktor
[TODO: ROLE-002]	Krankenschwester	Klinisch	Vollständige Patientenversorgung	EHR, Medikation	Pflegedienstleitung
[TODO: ROLE-003]	Medizinischer Assistent	Klinisch	Begrenzt	EHR (Vitalwerte, Terminplanung)	Klinischer Manager
[TODO: ROLE-004]	Abrechnungsspezialist	Abrechnung	Nur Abrechnungsdaten	Abrechnungssystem	Abrechnungsmanager

Rollen-ID	Rollenname	Abteilung	ePHI-Zugriffsstufe	Systeme	Genehmigung erforderlich
[TODO: ROLE-005]	IT-Administrator	IT	Systemadministrator	Alle Systeme	IT-Manager + Security Officer
[TODO: ROLE-006]	Rezeptionist	Empfang	Nur demografische Daten	EHR (Terminplanung)	Büroleiter

8.5.2 5.2 Zugriffsmatrix

Rolle	Patientendemografik	Klinische Notizen	Laborergebnisse	Medikamente	Abrechnung	Systemadministrator
Arzt	Lesen/Schreiben	Lesen/Schreiben	Lesen/Schreiben	Lesen/Schreiben	Lesen	Nein
Krankenschwester	Lesen/Schreiben	Lesen/Schreiben	Lesen	Lesen/Schreiben	Nein	Nein
Medizinischer Assistent	Lesen/Schreiben	Lesen	Lesen	Nein	Nein	Nein
Abrechnungsspezialist	Lesen	Nein	Nein	Nein	Lesen/Schreiben	Nein
IT-Administrator	Nein*	Nein*	Nein*	Nein*	Nein*	Ja
Rezeptionist	Lesen/Schreiben	Nein	Nein	Nein	Nein	Nein

*IT-Administratoren haben technischen Zugriff, sollten aber nicht auf ePHI zugreifen, es sei denn, dies ist für die Fehlerbehebung erforderlich

8.6 6. Schulungsanforderungen

8.6.1 6.1 Schulung zur Mitarbeitersicherheit

Erstschulung (Innerhalb von 30 Tagen nach Einstellung): - HIPAA-Überblick - Richtlinien zur Mitarbeitersicherheit - Zugriffskontrollverfahren - Passwortanforderungen - Vertraulichkeitsverpflichtungen - Sanktionen bei Verstößen

Jährliche Schulung: - Auffrischung zur Mitarbeitersicherheit - Richtlinienaktualisierungen - Fallstudien - Neue Bedrohungen

Rollenspezifische Schulung: - Vorgesetzte: Überwachungsverantwortlichkeiten - IT-Personal: Technische Schutzmaßnahmen - Manager: Verfahren zur Zugriffsgenehmigung

8.6.2 6.2 Schulungsdokumentation

Erforderliche Dokumentation: - Schulungsteilnahmeprotokolle - Schulungsmaterialien - Testergebnisse (falls zutreffend) - Bestätigung des Verständnisses - Schulungszertifikate

Aufbewahrung: [TODO: 6 Jahre]

8.7 7. Vertraulichkeitsvereinbarungen

8.7.1 7.1 Anforderungen an Vertraulichkeitsvereinbarungen

Alle Mitarbeiter müssen unterzeichnen: - Vertraulichkeitsvereinbarung - Richtlinie zur akzeptablen Nutzung - HIPAA-Bestätigung - Sicherheitsrichtlinienbestätigung

Zeitpunkt: - Vor Gewährung des Zugriffs auf ePHI - Bei Richtlinienänderungen (erneute Bestätigung) - Jährlich (erneute Bestätigung)

8.7.2 7.2 Vereinbarungsinhalt

Vertraulichkeitsvereinbarung muss enthalten: - Verpflichtung zum Schutz von PHI/ePHI - Verbot unbefugten Zugriffs - Verbot unbefugter Offenlegung - Meldepflichten für Vorfälle - Sanktionen bei Verstößen - Verpflichtungen bestehen nach Kündigung fort - Bestätigung des Verständnisses

Vereinbarungsspeicherung: [TODO: HR-Personalakten, elektronisches Repository]

8.8 8. Überwachung und Compliance

8.8.1 8.1 Überwachung der Mitarbeitersicherheit

Überwachungsaktivitäten: - Überprüfung von Zugriffsprotokollen - Untersuchungen unangemessenen Zugriffs - Audits zur Richtlinieneinhaltung - Verfolgung der Schulungsabschlüsse - Compliance bei Hintergrundprüfungen - Compliance bei Kündigungsverfahren

Überwachungshäufigkeit: | Aktivität | Häufigkeit | Verantwortlich | |————|————|————-| | Zugriffsprotokollprüfung | Monatlich | Security Officer | | Schulungs-Compliance | Vierteljährlich | HR + Privacy Officer | | Hintergrundprüfungs-Compliance | Jährlich | HR | | Kündigungsverfahrensaudit | Vierteljährlich | Security Officer |

8.8.2 8.2 Compliance-Metriken

Metrik	Ziel	Aktuell	Status
Schulungsabschlussrate	100%	[TODO: %]	[TODO: Grün/Gelb/Rot]
Hintergrundprüfungen abgeschlossen	100%	[TODO: %]	[TODO: Grün/Gelb/Rot]
Kündigungsverfahren befolgt	100%	[TODO: %]	[TODO: Grün/Gelb/Rot]
Zugriffsüberprüfungen abgeschlossen	100%	[TODO: %]	[TODO: Grün/Gelb/Rot]

8.9 9. Dokumentation und Aufzeichnungen

8.9.1 9.1 Erforderliche Dokumentation

- Zugriffsautorisierungsformulare
- Hintergrundprüfungsergebnisse

- Vertraulichkeitsvereinbarungen
- Schulungsunterlagen
- Kündigungs-Checklisten
- Überprüfung der Zugriffskündigung
- Überwachungsprotokolle
- Vorfallberichte

8.9.2 9.2 Aufbewahrung

Aufbewahrungsfrist: [TODO: 6 Jahre ab Beendigung des Arbeitsverhältnisses oder letztem Gültigkeitsdatum]

Speicherort: [TODO: HR-System, Dokumentenmanagementsystem]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 9

Einrichtungszugangskontrollen

Dokument-ID: HIPAA-0300
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

9.1 1. Zweck

Dieses Dokument beschreibt die Einrichtungszugangskontrollen für AdminSend GmbH, um den physischen Zugang zu elektronischen Informationssystemen und den Einrichtungen, in denen sie untergebracht sind, zu begrenzen und gleichzeitig ordnungsgemäß autorisierten Zugang zu ermöglichen.

9.1.1 1.1 HIPAA-Anforderung

Standard: §164.310(a)(1) - Facility Access Controls (Erforderlich)

Implementierungsspezifikationen: - §164.310(a)(2)(i) - Notfallbetrieb (Adressierbar) - §164.310(a)(2)(ii) - Einrichtungssicherheitsplan (Adressierbar) - §164.310(a)(2)(iii) - Zugriffskontroll- und Validierungsverfahren (Adressierbar) - §164.310(a)(2)(iv) - Wartungsaufzeichnungen (Adressierbar)

9.2 2. Einrichtungsinventar

9.2.1 2.1 Einrichtungen mit ePHI

Einrichtungs-ID	Einrichtungsname	Adresse	Typ	ePHI-Systeme	Zugriffsstufe
[TODO: FAC-001]	Hauptrechenzentrum	[TODO: Adresse]	Rechenzentrum	Alle Produktionssysteme	Eingeschränkt

Einrichtungs-ID	Einrichtungsname	Adresse	Typ	ePHI-Systeme	Zugriffsstufe
[TODO: FAC-002]	Hauptklinik	[TODO: Adresse]	Klinisch	EHR-Workstations	Kontrolliert
[TODO: FAC-003]	Verwaltungsbüro	[TODO: Adresse]	Büro	Abrechnungssysteme	Kontrolliert
[TODO: FAC-004]	Backup-Standort	[TODO: Adresse]	DR-Standort	Backup-Systeme	Eingeschränkt

9.2.2 2.2 Einrichtungsklassifizierung

Eingeschränkter Zugang: - Rechenzentren - Serverräume - Netzwerkgeräteräume - Backup-Speicherbereiche

Kontrollierter Zugang: - Klinische Bereiche - Verwaltungsbüros - Patientenaktenräume

Öffentlicher Zugang: - Wartezimmer - Öffentliche Korridore - Cafeteria

9.3 3. Notfallbetrieb

9.3.1 3.1 Notfallzugangsverfahren

Zweck: Verfahren festlegen, um Einrichtungszugang zur Unterstützung der Wiederherstellung verlorener Daten im Rahmen des Disaster-Recovery- und Notfallbetriebsplans zu ermöglichen.

Notfallszenarien: - Feuer oder Naturkatastrophe - Stromausfall - Systemausfall, der sofortigen Zugang erfordert - Sicherheitsvorfall, der Untersuchung erfordert

Notfallzugangsprozess: 1. **Autorisierung:** Security Officer oder Beauftragter autorisiert Notfallzugang 2. **Begleitung:** Notfallpersonal wird von autorisiertem Personal begleitet 3. **Dokumentation:** Aller Notfallzugang wird protokolliert 4. **Wiederherstellung:** Normale Zugangskontrollen nach Notfall wiederhergestellt 5. **Überprüfung:** Nachträgliche Überprüfung des Notfallzugangs

Notfallkontakte: | Rolle | Name | Telefon (24/7) | Backup | |——-|——|————-|——| | Security Officer | {{ meta.roles.security_officer.name }} | [TODO: Telefon] | [TODO: Backup-Name/Telefon] | | Facility Manager | [TODO: Name] | [TODO: Telefon] | [TODO: Backup] | | IT Manager | [TODO: Name] | [TODO: Telefon] | [TODO: Backup] |

9.3.2 3.2 Notfallzugangsausrüstung

Notfallzugangswerkzeuge: - Hauptschlüssel (gesichert in Notfallbox) - Zugangskarten (Notfall-Override) - Schlossumgehungswerkzeuge (nur autorisiertes Personal) - Notbeleuchtung - Kommunikationsgeräte

Speicherort: [TODO: Sicherer Ort mit dokumentiertem Zugang]

9.4 4. Einrichtungssicherheitsplan

9.4.1 4.1 Physische Sicherheitsmaßnahmen

Perimetersicherheit: - Zaun: [TODO: Ja/Nein, Beschreibung] - Tore: [TODO: Ja/Nein, Beschreibung] - Beleuchtung: [TODO: Beschreibung] - Beschilderung: [TODO: “Nur autorisiertes Personal”-

Schilder] - Landschaftsgestaltung: [TODO: Klare Sichtlinien]

Gebäudesicherheit: - Außentüren: [TODO: Anzahl, Schließmechanismen] - Fenster: [TODO: Sicherheitsmaßnahmen] - Ladedocks: [TODO: Sicherheitsmaßnahmen] - Dachzugang: [TODO: Sicherheitsmaßnahmen]

Innensicherheit: - Empfang/Sicherheitsschalter: [TODO: Ja/Nein, Öffnungszeiten] - Sicherheitspersonal: [TODO: Ja/Nein, Zeitplan] - Besucherverwaltung: [TODO: System/Prozess] - Begleitanforderungen: [TODO: Bereiche, die Begleitung erfordern]

Rechenzentrum/Serverraum-Sicherheit: - Dedizierter Raum: [TODO: Ja/Nein] - Verstärkte Wände: [TODO: Ja/Nein] - Doppelboden: [TODO: Ja/Nein] - Brandbekämpfung: [TODO: Typ] - Umgebungsüberwachung: [TODO: Temperatur, Luftfeuchtigkeit] - Wassererkennung: [TODO: Ja/Nein] - Notstromversorgung: [TODO: USV, Generator]

9.4.2 4.2 Zugriffskontrollsysteme

Physisches Zugriffskontrollsystem: - **Systemtyp:** [TODO: Kartenleser, biometrisch, Tastenfeld] - **Anbieter:** [TODO: Anbietername] - **Abdeckung:** [TODO: Abgedeckte Türen/Bereiche] - **Überwachung:** [TODO: 24/7-Überwachung, Alarme]

Zugriffskontrollfunktionen: - Individuelle Identifikation - Zeitbasierte Zugriffsbeschränkungen - Bereichsbasierte Zugriffsbeschränkungen - Anti-Passback - Audit-Protokollierung - Echtzeitalarme

Zugangskartenverwaltung: - Kartenausgabeprozess - Kartendeaktivierungsprozess - Verfahren bei verlorenen/gestohlenen Karten - Kartenrückgabe bei Kündigung

9.4.3 4.3 Überwachungssysteme

Videoüberwachung: - **Abdeckung:** [TODO: Eingänge, Ausgänge, Serverräume usw.] - **Kameratyp:** [TODO: Fest, PTZ, Auflösung] - **Aufzeichnung:** [TODO: Kontinuierlich, bewegungsaktiviert] - **Aufbewahrung:** [TODO: Tage/Monate] - **Überwachung:** [TODO: Live-Überwachung, Überprüfungszeitplan]

Überwachungsstandorte: | Standort | Kameraanzahl | Aufzeichnung | Aufbewahrung | Zweck | |———-|————|————|————|——-| | [TODO: Haupteingang] | [TODO: 2] | Kontinuierlich | [TODO: 90 Tage] | Zugangsüberwachung | | [TODO: Serverraum] | [TODO: 1] | Kontinuierlich | [TODO: 90 Tage] | Sicherheitsüberwachung | | [TODO: Parkplatz] | [TODO: 4] | Bewegung | [TODO: 30 Tage] | Perimetersicherheit |

9.5 5. Zugriffskontroll- und Validierungsverfahren

9.5.1 5.1 Zugriffsautorisierung

Autorisierungsprozess: 1. **Anfrage:** Manager reicht Zugriffsanfrage ein 2. **Begründung:** Geschäftlicher Bedarf dokumentiert 3. **Genehmigung:** Security Officer genehmigt 4. **Bereitstellung:** Facility Manager stellt Zugriff bereit 5. **Dokumentation:** Zugriff im System protokolliert 6. **Benachrichtigung:** Mitarbeiter über gewährten Zugriff benachrichtigt

Zugriffsstufen: | Stufe | Beschreibung | Erforderliche Autorisierung | Zugängliche Bereiche | |——-|————|————————-|————————-| | Stufe 1 - Öffentlich | Allgemeine Öffentlichkeit | Keine | Wartebereiche, öffentliche Korridore | | Stufe 2 - Mitarbeiter | Reguläre Mitarbeiter |

Manager-Genehmigung | Bürobereiche, Pausenräume | | Stufe 3 - Klinisch | Klinisches Personal | Manager + Privacy Officer | Klinische Bereiche, Patientenakten | | Stufe 4 - IT | IT-Personal | IT-Manager + Security Officer | Serverräume, Netzwerkschränke | | Stufe 5 - Führungsebene | Führungszugang | CEO-Genehmigung | Alle Bereiche |

9.5.2 5.2 Besucherverwaltung

Besucherverfahren: 1. **Check-in:** Besucher meldet sich am Empfang an 2. **Identifikation:** Lichtbildausweis erforderlich und aufgezeichnet 3. **Ausweis:** Besucherausweis ausgestellt 4. **Begleitung:** Besucher wird in eingeschränkten Bereichen jederzeit begleitet 5. **Protokoll:** Besuch protokolliert (Name, Firma, Zweck, Zeit ein/aus, Gastgeber) 6. **Check-out:** Besucher gibt Ausweis zurück und meldet sich ab

Besuchertypen: - Lieferanten/Auftragnehmer - Business Associates - Auditoren - Gäste - Lieferpersonal

Besucherausweis: Deutlich mit "BESUCHER" gekennzeichneter Ausweis, andere Farbe als Mitarbeiterausweise

9.5.3 5.3 Zugriffvalidierung

Zugriffsüberprüfungsprozess: - **Häufigkeit:** Vierteljährlich - **Prüfer:** Facility Manager + Security Officer - **Umfang:** Alle aktiven Zugriffsberechtigungen - **Maßnahmen:** Unnötigen Zugriff widerrufen, Aufzeichnungen aktualisieren

Zugriffvalidierungs-Checkliste: - [ ] Überprüfen, ob Mitarbeiter noch Zugriff benötigt - [ ] Überprüfen, ob Zugriffsstufe für Rolle angemessen ist - [ ] Überprüfen, dass keine gekündigten Mitarbeiter aktiven Zugriff haben - [ ] Überprüfen, dass kein abgelaufener temporärer Zugriff besteht - [ ] Zugriffsdokumentation aktualisieren

9.5.4 5.4 Zugriffskündigung

Kündigungsprozess: 1. **Benachrichtigung:** HR benachrichtigt Facility Manager und Security Officer 2. **Sofortiger Widerruf:** Zugriff wird sofort bei Kündigung widerrufen 3. **Ausweiseinsammlung:** Mitarbeiterausweis eingesammelt 4. **Schlüsseleinsammlung:** Alle Schlüssel eingesammelt 5. **Überprüfung:** Zugriffskündigung im System überprüft 6. **Dokumentation:** Kündigung protokolliert

Kündigungs-Checkliste: - [ ] Zugangskarte deaktiviert - [ ] Schlüssel zurückgegeben - [ ] Alarmcodes geändert (falls zutreffend) - [ ] Besucherbegleitrechte widerrufen - [ ] Dokumentation aktualisiert

9.6 6. Wartungsaufzeichnungen

9.6.1 6.1 Einrichtungswartung

Wartungsaktivitäten: - Wartung des Zugriffskontrollsystems - Wartung des Überwachungssystems - Schloss- und Schlüsselwartung - Alarmsystemwartung - Brandbekämpfungssystemwartung - Wartung der Umgebungskontrollen - Notbeleuchtungswartung

Wartungsplan: | System | Wartungstyp | Häufigkeit | Anbieter | Letzter Service | Nächster Service | |———|————-|———|———-|—————|—————| | [TODO: Zugriffskontrolle] |

Präventiv | Vierteljährlich | [TODO: Anbieter] | [TODO: Datum] | [TODO: Datum] | | [TODO: Überwachung] | Präventiv | Halbjährlich | [TODO: Anbieter] | [TODO: Datum] | [TODO: Datum] | | [TODO: Brandbekämpfung] | Inspektion | Jährlich | [TODO: Anbieter] | [TODO: Datum] | [TODO: Datum] |

9.6.2 6.2 Wartungsdokumentation

Erforderliche Dokumentation: - Wartungsarbeitsaufträge - Serviceberichte - Ersetzte Teile - Durchgeführte Systemtests - Technikerqualifikationen - Zugriffsprotokolle für Wartungspersonal

Aufbewahrung: [TODO: 6 Jahre]

9.6.3 6.3 Wartungszugriffskontrolle

Anbieterzugang: - Anbieter wird während Wartung begleitet - Anbieterzugang wird protokolliert - Anbieterqualifikationen werden überprüft - Hintergrundprüfungen für reguläre Anbieter - Business Associate Agreement (falls PHI-Zugriff möglich)

9.7 7. Physische Sicherheitsvorfälle

9.7.1 7.1 Vorfalltypen

- Unbefugter Einrichtungszugang
- Tailgating
- Verlorene/gestohlene Zugangskarten oder Schlüssel
- Gewaltsamer Zutritt
- Manipulation des Überwachungssystems
- Alarmsystemausfälle

9.7.2 7.2 Vorfallreaktion

Reaktionsprozess: 1. **Erkennung:** Vorfall erkannt (Alarm, Beobachtung, Meldung) 2. **Benachrichtigung:** Security Officer sofort benachrichtigt 3. **Bewertung:** Schweregrad und Auswirkung bewerten 4. **Eindämmung:** Bereich sichern, Zugriffscodes bei Bedarf ändern 5. **Untersuchung:** Protokolle, Überwachungsaufnahmen überprüfen 6. **Behebung:** Korrekturmaßnahmen umsetzen 7. **Dokumentation:** Vorfall und Reaktion dokumentieren 8. **Überprüfung:** Nachträgliche Überprüfung und Lessons Learned

9.7.3 7.3 Vorfallprotokoll

Vorfall-ID	Datum	Typ	Standort	Beschreibung	Reaktion	Status
[TODO: INC-001]	[TODO: Datum]	[TODO: Typ]	[TODO: Standort]	[TODO: Beschreibung]	[TODO: Ergriffene Maßnahmen]	[TODO: Geschlossen]

9.8 8. Dokumentation und Aufzeichnungen

9.8.1 8.1 Erforderliche Dokumentation

- Einrichtungssicherheitsplan
- Zugriffsautorisierungsaufzeichnungen
- Besucherprotokolle
- Zugriffsüberprüfungsaufzeichnungen
- Wartungsaufzeichnungen
- Vorfallberichte
- Überwachungsaufnahmen (gemäß Aufbewahrungsrichtlinie)

9.8.2 8.2 Aufbewahrung

Aufbewahrungsfrist: [TODO: 6 Jahre ab Erstellung oder letztem Gültigkeitsdatum]

Speicherort: [TODO: Dokumentenmanagementsystem-Standort]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 10

Arbeitsplatznutzung und -sicherheit

Dokument-ID: HIPAA-0310
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

10.1 1. Zweck

Dieses Dokument beschreibt die Richtlinien zur Arbeitsplatznutzung und Arbeitsplatzsicherheit für AdminSend GmbH, um ordnungsgemäße auszuführende Funktionen, die Art und Weise ihrer Ausführung und physische Attribute der Umgebung von Arbeitsplätzen festzulegen, die auf ePHI zugreifen.

10.1.1 1.1 HIPAA-Anforderungen

Standard: §164.310(b) - Workstation Use (Erforderlich)
Standard: §164.310(c) - Workstation Security (Erforderlich)

10.2 2. Arbeitsplatznutzung

10.2.1 2.1 Arbeitsplatzdefinition

Arbeitsplatz: Ein elektronisches Computergerät (z.B. Laptop, Desktop-Computer, Tablet, Smartphone) und seine elektronischen Medien, die zum Zugriff auf, Erstellen, Empfangen, Verwalten oder Übertragen von ePHI verwendet werden.

Arbeitsplatztypen: - Desktop-Computer - Laptop-Computer - Tablets - Smartphones - Thin Clients - Workstations on Wheels (WOWs) - Kioske

10.2.2 2.2 Autorisierte Nutzung

Zulässige Verwendungen: - Zugriff auf ePHI für Behandlung, Zahlung oder Gesundheitsoperationen - Erstellen und Pflegen von Patientenakten - Kommunikation mit Patienten und Gesundheitsteam - Abrechnungs- und Verwaltungsfunktionen - Autorisierte Forschungsaktivitäten

Verbotene Verwendungen: - Persönliche Nutzung (außer minimaler gelegentlicher Nutzung) - Zugriff auf ePHI ohne Autorisierung - Weitergabe von Anmeldedaten - Installation nicht autorisierter Software - Anschluss nicht autorisierter Geräte - Zugriff auf unangemessene Websites - Herunterladen nicht autorisierter Dateien

10.2.3 2.3 Benutzerverantwortlichkeiten

Mitarbeiter müssen: - Arbeitsplätze nur für autorisierte Zwecke verwenden - Anmeldedaten schützen - Arbeitsplatz sperren beim Verlassen (auch kurz) - Abmelden nach Beendigung - Verlorene, gestohlene oder kompromittierte Arbeitsplätze sofort melden - Arbeitsplatzsoftware aktuell halten - Arbeitsplätze nicht ohne ordnungsgemäße Abmeldung/Anmeldung teilen - Bildschirme positionieren, um unbefugte Einsicht zu verhindern - Sichtschutzfilter in öffentlichen Bereichen verwenden

10.3 3. Arbeitsplatzsicherheit

10.3.1 3.1 Physische Sicherheit

Arbeitsplatzpositionierung: - Positionierung zur Minimierung unbefugter Einsicht - Vermeidung der Platzierung in der Nähe von Fenstern oder öffentlichen Bereichen - Sicherstellung angemessener physischer Sicherheit des Standorts - Berücksichtigung von Verkehrsmustern und Sichtbarkeit

Physische Sicherheitskontrollen: - Kabelschlösser für Laptops - Verschlossene Büros oder gesicherte Bereiche - Sichtschutzfilter - Automatische Bildschirmsperren - Physische Barrieren (Wände, Trennwände)

Mobile Arbeitsplätze: - Laptoptaschen, die Inhalt nicht identifizieren - Niemals unbeaufsichtigt in Fahrzeugen lassen - Hotelsafes bei Reisen verwenden - Alle mobilen Geräte verschlüsseln - Remote-Wipe-Funktion aktivieren

10.3.2 3.2 Technische Sicherheit

Authentifizierung: - Eindeutige Benutzer-ID erforderlich - Starkes Passwort oder biometrische Authentifizierung - Multi-Faktor-Authentifizierung (für Fernzugriff) - Keine gemeinsam genutzten Konten

Automatische Abmeldung/Sperre: - Bildschirmsperre nach [TODO: 5-15] Minuten Inaktivität - Automatische Abmeldung nach [TODO: 30] Minuten Inaktivität - Erneute Authentifizierung zum Fortsetzen erforderlich

Verschlüsselung: - Vollständige Festplattenverschlüsselung für alle Arbeitsplätze erforderlich - Verschlüsselungsstandard: [TODO: AES-256 oder gleichwertig] - Verfahren zur Verschlüsselungsschlüsselverwaltung

Antivirus/Anti-Malware: - Endpoint-Protection-Software erforderlich - Echtzeit-Scanning aktiviert - Automatische Updates aktiviert - Regelmäßige Scans geplant

Firewall: - Host-basierte Firewall aktiviert - Standard-Ablehnung eingehender Verbindungen - Nur autorisierte Anwendungen erlaubt

Software-Updates: - Betriebssystem-Patches innerhalb von [TODO: 30] Tagen angewendet - Kritische Sicherheitspatches innerhalb von [TODO: 7] Tagen angewendet - Anwendungsupdates gemäß Herstellerempfehlungen angewendet

10.3.3 3.3 Konfigurationsstandards

Basiskonfiguration: - Genehmigte Betriebssystemversion - Nur genehmigte Anwendungen - Unnötige Dienste deaktiviert - Standardpasswörter geändert - Administratorrechte eingeschränkt - Audit-Protokollierung aktiviert

Konfigurationsverwaltung: - Standard-Images für Arbeitsplatzbereitstellung - Konfigurationsänderungen dokumentiert und genehmigt - Regelmäßige Konfigurationsaudits - Nicht konforme Arbeitsplätze behoben

10.4 4. Arbeitsplatzinventar

10.4.1 4.1 Asset-Inventar

Asset-ID	Typ	Standort	Benutzer	ePHI-Zugriff	Verschlüsselung	Letztes Update
[TODO: WS-001]	Desktop	[TODO: Büro 101]	[TODO: Benutzername]	Ja	Ja	[TODO: Datum]
[TODO: WS-002]	Laptop	[TODO: Mobil]	[TODO: Benutzername]	Ja	Ja	[TODO: Datum]
[TODO: WS-003]	Tablet	[TODO: Klinik A]	[TODO: Geteilt]	Ja	Ja	[TODO: Datum]

10.4.2 4.2 Asset-Tracking

Tracking-Anforderungen: - Asset-Tag/ID - Seriennummer - Hersteller und Modell - Zugewiesener Benutzer - Standort - ePHI-Zugriff (Ja/Nein) - Verschlüsselungsstatus - Letztes Sicherheitsupdate - Garantie-/Support-Ablauf

Inventaraktualisierungen: - Neue Arbeitsplatzbereitstellung - Arbeitsplatzneuzuweisung - Arbeitsplatzstilllegung - Standortänderungen - Vierteljährliche Inventarüberprüfung

10.5 5. Arbeitsplatz-Lebenszyklus

10.5.1 5.1 Beschaffung

Beschaffungsanforderungen: - Erfüllung minimaler Sicherheitsstandards - Kompatibilität mit Sicherheitssoftware - Unterstützung vollständiger Festplattenverschlüsselung - Von IT-Abteilung genehmigt - Angemessene Garantie/Support enthalten

Genehmigungsprozess: 1. Abteilung reicht Anfrage ein 2. IT prüft technische Anforderungen 3. Security Officer genehmigt Sicherheitsfunktionen 4. Beschaffung bearbeitet Bestellung

10.5.2 5.2 Bereitstellung

Bereitstellungsprozess: 1. **Imaging:** Standard-Image installieren 2. **Konfiguration:** Sicherheitskonfiguration anwenden 3. **Verschlüsselung:** Vollständige Festplattenverschlüsselung aktivieren 4. **Software:** Erforderliche Anwendungen installieren 5. **Testen:** Funktionalität und Sicherheit überprüfen 6. **Dokumentation:** Zum Asset-Inventar hinzufügen 7. **Zuweisung:** Benutzer zuweisen 8. **Schulung:** Benutzerschulung bereitstellen 9. **Bestätigung:** Benutzer unterzeichnet Nutzungsvereinbarung

10.5.3 5.3 Wartung

Wartungsaktivitäten: - Software-Updates und Patches - Antivirus-Updates - Hardware-Reparaturen - Leistungsoptimierung - Sicherheitsscans

Wartungsplan: | Aktivität | Häufigkeit | Verantwortlich | |————|————|————-| | OS-Patches | Monatlich | IT | | Antivirus-Updates | Täglich (automatisch) | Endpoint Protection | | Sicherheitsscans | Wöchentlich | IT Security | | Hardware-Inspektion | Jährlich | IT |

10.5.4 5.4 Stilllegung/Entsorgung

Stilllegungsprozess: 1. **Außerbetriebnahme:** Aus Produktion entfernen 2. **Datenlöschung:** Alle Daten sicher löschen 3. **Überprüfung:** Datenvernichtung überprüfen 4. **Dokumentation:** Entsorgung dokumentieren 5. **Physische Vernichtung:** Speichermedien vernichten (falls erforderlich) 6. **Zertifikat:** Vernichtungszertifikat einholen 7. **Inventaraktualisierung:** Aus Asset-Inventar entfernen

Datenlöschungsmethoden: - Softwarebasiertes Löschen (NIST 800-88-konform) - Entmagnetisierung (für magnetische Medien) - Physische Vernichtung (Schreddern, Zerkleinern)

Löschungsstandards: - Mindestens 3-faches Überschreiben - Überprüfung der Löschung - Dokumentation der verwendeten Methode - Vernichtungszertifikat aufbewahrt

10.6 6. Fernzugriffs-Arbeitsplätze

10.6.1 6.1 Fernzugriffsanforderungen

Fernzugriffsszenarien: - Arbeit von zu Hause - Telemedizin - Mobile Kliniker - Geschäftsreisen - Notfallzugriff

Sicherheitsanforderungen: - VPN für allen Fernzugriff erforderlich - Multi-Faktor-Authentifizierung erforderlich - Nur verschlüsselte Verbindungen - Nur firmeneigene oder genehmigte Geräte - Einhaltung aller Arbeitsplatzsicherheitsrichtlinien

10.6.2 6.2 Heimbüro-Sicherheit

Heimbüro-Anforderungen: - Dedizierter Arbeitsbereich (falls möglich) - Physische Sicherheit (verschlossener Raum/Bereich) - Sicheres WLAN (WPA3 oder WPA2) - Keine gemeinsame Computernutzung - Privatsphäre vor Familienmitgliedern - Sichere Dokumentenaufbewahrung

Heimnetzwerksicherheit: - Standard-Router-Passwort ändern - Router-Firewall aktivieren - WPS deaktivieren - Starkes WLAN-Passwort verwenden - Router-Firmware aktuell halten - Separates Gästenetzwerk

10.7 7. Gemeinsam genutzte Arbeitsplätze

10.7.1 7.1 Richtlinie für gemeinsam genutzte Arbeitsplätze

Szenarien für gemeinsam genutzte Arbeitsplätze: - Klinische Workstations on Wheels (WOWs) - Pflegestationscomputer - Kioske - Konferenzraumcomputer

Sicherheitsanforderungen: - Individuelle Anmeldung erforderlich (keine gemeinsamen Konten) - Automatische Abmeldung nach Inaktivität - Clear-Screen-Richtlinie (Abmeldung zwischen Benutzern) - Physische Sicherheit des Standorts - Regelmäßige Reinigung und Wartung

10.7.2 7.2 Kiosk-Modus

Kiosk-Konfiguration: - Begrenzte Funktionalität - Eingeschränkter Anwendungszugriff - Keine lokale Datenspeicherung - Automatisches Sitzungs-Timeout - Automatische Rückkehr zum Anmeldebildschirm - Manipulationssichere Hardware

10.8 8. Mobile Device Management (MDM)

10.8.1 8.1 MDM-Anforderungen

MDM-Funktionen: - Remote-Wipe - Verschlüsselungsdurchsetzung - Passwortrichtliniendurchsetzung - Anwendungsverwaltung - Geräte-Compliance-Überwachung - Standortverfolgung (falls zulässig)

MDM-Registrierung: - Alle mobilen Geräte mit ePHI-Zugriff müssen registriert werden - Registrierung vor Gewährung des ePHI-Zugriffs - Benutzerbestätigung der MDM-Funktionen

10.8.2 8.2 BYOD (Bring Your Own Device)

BYOD-Richtlinie: [TODO: Erlaubt/Nicht erlaubt]

Falls BYOD erlaubt: - MDM-Registrierung erforderlich - Containerisierung von Arbeitsdaten - Trennung von Arbeits-/Privatdaten - Remote-Wipe nur von Arbeitsdaten - Benutzervereinbarung mit Bestätigung von MDM - Einhaltung aller Sicherheitsrichtlinien

10.9 9. Vorfallreaktion

10.9.1 9.1 Arbeitsplatzvorfälle

Vorfalltypen: - Verlorener oder gestohlener Arbeitsplatz - Malware-Infektion - Unbefugter Zugriff - Physischer Schaden - Datenschutzverletzung - Richtlinienverstoß

10.9.2 9.2 Meldeverfahren

Sofortige Meldung erforderlich: 1. **Melden:** Sofort an IT-Helpdesk und Security Officer melden 2. **Deaktivieren:** IT deaktiviert Fernzugriff und Netzwerkzugriff 3. **Bewerten:** Security Officer bewertet Vorfall 4. **Eindämmen:** Vorfall eindämmen (Remote-Wipe falls erforderlich) 5. **Untersuchen:** Umfang und Auswirkung untersuchen 6. **Beheben:** Korrekturmaßnahmen umsetzen 7. **Dokumentieren:** Vorfall und Reaktion dokumentieren 8. **Nachbereitung:** Nachträgliche Überprüfung durchführen

Kontaktinformationen: - IT-Helpdesk: [TODO: Telefon/E-Mail] - Security Officer: {{ meta.roles.security_officer.email }} - Nach Geschäftsschluss: [TODO: Notfallkontakt]

10.10 10. Schulung und Sensibilisierung

10.10.1 10.1 Schulungsanforderungen

Erstschulung: - Arbeitsplatznutzungsrichtlinie - Arbeitsplatzsicherheitsanforderungen - Physische Sicherheitsmaßnahmen - Vorfallmeldung - Richtlinie zur akzeptablen Nutzung

Jährliche Schulung: - Richtlinienauffrischung - Neue Bedrohungen - Best Practices - Fallstudien

Just-in-Time-Schulung: - Neue Arbeitsplatzbereitstellung - Richtlinienänderungen - Nach Sicherheitsvorfällen

10.10.2 10.2 Sensibilisierungsaktivitäten

- Sicherheitserinnerungen (E-Mail, Poster)
- Bildschirmsperr-Erinnerungen
- Clean-Desk-Richtlinienerinnerungen
- Phishing-Sensibilisierung
- Social-Engineering-Sensibilisierung

10.11 11. Überwachung und Compliance

10.11.1 11.1 Compliance-Überwachung

Überwachungsaktivitäten: - Arbeitsplatzkonfigurationsaudits - Verschlüsselungs-Compliance-Prüfungen - Software-Update-Compliance - Antivirus-Statusprüfungen - Physische Sicherheitsinspektionen - Richtlinien-Compliance-Audits

Überwachungshäufigkeit: | Aktivität | Häufigkeit | Verantwortlich | |————|————|————-| | Konfigurationsaudit | Vierteljährlich | IT Security | | Verschlüsselungsprüfung | Monatlich | IT Security | | Update-Compliance | Wöchentlich | IT | | Physische Inspektion | Halbjährlich | Facilities + IT |

10.11.2 11.2 Nicht-Compliance

Nicht-Compliance-Maßnahmen: 1. **Identifikation:** Nicht-konformer Arbeitsplatz identifiziert 2. **Benachrichtigung:** Benutzer benachrichtigt 3. **Behebung:** Benutzer erhält Zeitrahmen zur Behebung 4. **Eskalation:** Eskalieren, falls nicht behoben 5. **Einschränkung:** ePHI-Zugriff bei Bedarf einschränken 6. **Sanktionen:** Sanktionen gemäß Richtlinie anwenden

10.12 12. Dokumentation und Aufzeichnungen

10.12.1 12.1 Erforderliche Dokumentation

- Arbeitsplatzinventar
- Konfigurationsstandards
- Bereitstellungsaufzeichnungen

- Wartungsaufzeichnungen
- Entsorgungs-/Löschungszertifikate
- Vorfallberichte
- Schulungsunterlagen
- Compliance-Audit-Ergebnisse

10.12.2 12.2 Aufbewahrung

Aufbewahrungsfrist: [TODO: 6 Jahre ab Stilllegung/Entsorgung]

Speicherort: [TODO: Asset-Management-System, Dokumenten-Repository]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 11

Zugangskontrolle

Dokument-ID: HIPAA-0400
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

11.1 1. Zweck

Dieses Dokument beschreibt die technischen Schutzmaßnahmen zur Zugangskontrolle für AdminSend GmbH, um technische Richtlinien und Verfahren für elektronische Informationssysteme zu implementieren, die ePHI verwalten, um nur autorisierten Personen oder Softwareprogrammen Zugang zu gewähren.

11.1.1 1.1 HIPAA-Anforderung

Standard: §164.312(a)(1) - Access Control (Erforderlich)

Implementierungsspezifikationen: - §164.312(a)(2)(i) - Eindeutige Benutzeridentifikation (Erforderlich) - §164.312(a)(2)(ii) - Notfallzugangsverfahren (Erforderlich) - §164.312(a)(2)(iii) - Automatische Abmeldung (Adressierbar) - §164.312(a)(2)(iv) - Verschlüsselung und Entschlüsselung (Adressierbar)

11.2 2. Eindeutige Benutzeridentifikation

11.2.1 2.1 Benutzer-ID-Anforderungen

Anforderung: Zuweisung eines eindeutigen Namens und/oder einer Nummer zur Identifizierung und Verfolgung der Benutzeridentität.

Benutzer-ID-Standards: - Eindeutig für jeden einzelnen Benutzer - Nicht zwischen Benutzern geteilt - Nach Kündigung nicht wiederverwendet - Format: [TODO: vorname.nachname, Mitarbeiter-ID usw.] - Mindestlänge: [TODO: 6 Zeichen]

Verbotene Praktiken: - Gemeinsam genutzte Konten - Generische Konten (außer für spezifische genehmigte Zwecke) - Standardkonten (müssen deaktiviert oder umbenannt werden) - Gastkonten (müssen deaktiviert werden)

11.2.2 2.2 Benutzerkontenverwaltung

Kontoerstellungsprozess: 1. Manager reicht Zugriffsanfrage ein 2. HR überprüft Beschäftigungsstatus 3. Security Officer genehmigt basierend auf Rolle 4. IT erstellt eindeutiges Benutzerkonto 5. Benutzer über Kontoerstellung benachrichtigt 6. Benutzer schließt erste Anmeldung und Passworteinrichtung ab

Kontotypen: | Kontotyp | Zweck | Erforderliche Genehmigung | Überwachung | |———-|———-|———————-|————-| | Standardbenutzer | Reguläres Mitglied | Manager | Standard | | Privilegierter Benutzer | Systemadministration | IT-Manager + Security Officer | Erweitert | | Dienstkonto | Automatisierte Prozesse | Security Officer | Erweitert | | Notfallzugang | Break-Glass-Zugang | Security Officer | Sofortige Überprüfung |

11.2.3 2.3 Authentifizierungsmethoden

Primäre Authentifizierung: - Benutzername und Passwort - Mindestpasswortanforderungen: - Länge: [TODO: 12 Zeichen Minimum] - Komplexität: Groß-, Kleinbuchstaben, Zahl, Sonderzeichen - Historie: [TODO: 12 vorherige Passwörter gespeichert] - Alter: Maximum [TODO: 90 Tage], Minimum [TODO: 1 Tag] - Sperrung: [TODO: 5 fehlgeschlagene Versuche], Sperrdauer [TODO: 30 Minuten]

Multi-Faktor-Authentifizierung (MFA): - Erforderlich für: Fernzugriff, privilegierte Konten, ePHI-Zugriff aus nicht vertrauenswürdigen Netzwerken - Methoden: SMS-Code, Authenticator-App, Hardware-Token, biometrisch - Backup-Codes für MFA-Wiederherstellung bereitgestellt

Single Sign-On (SSO): - Zentralisierte Authentifizierung - Reduziert Passwortmüdigkeit - Audit-Trail des Zugriffs - Integration mit MFA

11.3 3. Notfallzugangsverfahren

11.3.1 3.1 Notfallzugangsdefinition

Notfallsituationen: - Systemausfall, der normale Authentifizierung verhindert - Naturkatastrophe - Cyberangriff, der sofortige Reaktion erfordert - Lebensbedrohliche Patientensituation, die sofortigen ePHI-Zugriff erfordert - Kritische Systemwartung

11.3.2 3.2 Break-Glass-Konten

Break-Glass-Konto-Eigenschaften: - Hochprivilegierter Zugriff - Nur in Notfällen verwendet - Anmeldedaten gesichert (versiegelter Umschlag, Passworttresor) - Sofortige Benachrichtigung bei Verwendung - Automatische Protokollierung aller Aktivitäten - Sofortige Überprüfung erforderlich

Break-Glass-Konto-Inventar: | Konto-ID | System | Zugriffsstufe | Anmeldedatenspeicherort | Zuletzt verwendet | Überprüft von | |———-|——|————|——————-|————-|————| | [TODO: BG-001] | Active Directory | Domain Admin | [TODO: Sicherer Tresor] | [TODO: Datum] | [TODO: Security Officer] | | [TODO: BG-002] | EHR-System | System Admin | [TODO: Sicherer Tresor] | [TODO: Datum] | [TODO: Security Officer] |

11.3.3 3.3 Notfallzugangsprozess

Prozessschritte: 1. **Feststellung:** Notfallsituation festgestellt 2. **Autorisierung:** Security Officer oder Beauftragter autorisiert Notfallzugang 3. **Zugriff:** Break-Glass-Anmeldedaten verwenden 4. **Protokollierung:** Alle Aktivitäten automatisch protokolliert 5. **Benachrichtigung:** Security Officer sofort benachrichtigt 6. **Überwachung:** Echtzeitüberwachung der Notfallzugriffsaktivitäten 7. **Überprüfung:** Sofortige Überprüfung nach Zugriff 8. **Dokumentation:** Notfall, ergriffene Maßnahmen, Begründung dokumentieren 9. **Anmeldedatenrotation:** Break-Glass-Anmeldedaten nach Verwendung ändern

Notfallzugriffsprotokoll: | Datum/Zeit | Benutzer | System | Grund | Autorisiert von | Ergriffene Maßnahmen | Überprüfungsdatum | |————|———-|——|——-|————|—————-|————-| | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

11.4 4. Automatische Abmeldung

11.4.1 4.1 Anforderungen an automatische Abmeldung

Anforderung: Implementierung elektronischer Verfahren, die eine elektronische Sitzung nach einer vorbestimmten Zeit der Inaktivität beenden.

Begründung: Unbefugten Zugriff auf ePHI verhindern, wenn Arbeitsplatz unbeaufsichtigt gelassen wird.

11.4.2 4.2 Timeout-Einstellungen

Inaktivitäts-Timeouts: | System/Anwendung | Timeout-Zeitraum | Aktion | Override erlaubt | |———————|———————|——|———————| | Arbeitsplätze | [TODO: 15 Minuten] | Bildschirmsperre | Nein | | EHR-System | [TODO: 10 Minuten] | Sitzungs-Timeout | Nein | | Webanwendungen | [TODO: 20 Minuten] | Sitzungs-Timeout | Nein | | VPN | [TODO: 30 Minuten] | Trennen | Nein | | Mobile Geräte | [TODO: 5 Minuten] | Bildschirmsperre | Nein |

Timeout-Aktionen: - **Bildschirmsperre:** Passwort zum Entsperren erforderlich, Sitzung bleibt aktiv - **Sitzungs-Timeout:** Beendet Sitzung, erneute Authentifizierung erforderlich - **Trennen:** Beendet Netzwerkverbindung

11.4.3 4.3 Implementierung

Technische Implementierung: - Gruppenrichtlinie (Windows) - Konfigurationsprofile (macOS, iOS) - Anwendungsebenen-Timeouts - Netzwerkebenen-Timeouts (VPN, Firewall)

Benutzerbenachrichtigung: - Warnung vor Timeout (z.B. 2 Minuten) - Klare Anzeige des gesperrten Zustands - Anweisungen zum Entsperren

11.5 5. Verschlüsselung und Entschlüsselung

11.5.1 5.1 Verschlüsselungsanforderungen

Anforderung: Implementierung eines Mechanismus zur Verschlüsselung und Entschlüsselung von ePHI.

Verschlüsselungsanwendungsfälle: - ePHI im Ruhezustand (gespeicherte Daten) - ePHI in Übertragung (übertragene Daten) - Backup-Medien - Mobile Geräte - Wechselmedien - E-Mail mit ePHI

11.5.2 5.2 Verschlüsselungsstandards

Genehmigte Verschlüsselungsalgorithmen: - **Symmetrisch:** AES-256, AES-128 - **Asymmetrisch:** RSA-2048 oder höher, ECC - **Hashing:** SHA-256, SHA-512 - **TLS:** TLS 1.2 oder höher

Verbotene Algorithmen: - DES, 3DES - MD5, SHA-1 - SSL, TLS 1.0, TLS 1.1 - RC4

11.5.3 5.3 Verschlüsselung im Ruhezustand

Vollständige Festplattenverschlüsselung: - Alle Arbeitsplätze und Laptops: [TODO: BitLocker, FileVault, LUKS] - Alle Server mit ePHI: [TODO: BitLocker, dm-crypt] - Alle mobilen Geräte: [TODO: Native Geräteverschlüsselung]

Datenbankverschlüsselung: - Transparent Data Encryption (TDE) für Datenbanken - Spaltenebenen-Verschlüsselung für sensible Felder - Verschlüsselungsschlüsselverwaltung

Datei-/Ordnerverschlüsselung: - Verschlüsselte Dateisysteme - Verschlüsselte Container - Dokumentenebenen-Verschlüsselung

11.5.4 5.4 Verschlüsselung in Übertragung

Netzwerkverschlüsselung: - TLS 1.2+ für allen Webverkehr - VPN für Fernzugriff (IPsec, SSL VPN) - Verschlüsselte E-Mail (S/MIME, PGP) - SFTP/SCP für Dateiübertragungen (kein FTP) - HTTPS für alle Webanwendungen

Drahtlosverschlüsselung: - WPA3 oder WPA2-Enterprise - Kein WEP oder offene Netzwerke - Zertifikatbasierte Authentifizierung

11.5.5 5.5 Schlüsselverwaltung

Schlüsselverwaltungs-Lebenszyklus: 1. **Generierung:** Kryptografisch sichere Zufallsgenerierung 2. **Verteilung:** Sichere Schlüsselverteilungsmechanismen 3. **Speicherung:** Hardware Security Module (HSM) oder sicherer Schlüsseltresor 4. **Rotation:** Regelmäßiger Schlüsselrotationsplan 5. **Backup:** Sichere Sicherung von Verschlüsselungsschlüsseln 6. **Vernichtung:** Sichere Vernichtung, wenn nicht mehr benötigt

Schlüsselverwaltungssystem: - Zentralisierte Schlüsselverwaltung - Zugriffskontrollen auf Schlüssel - Audit-Protokollierung des Schlüsselzugriffs - Schlüsselhinterlegungs-/Wiederherstellungsverfahren

Schlüsselrotationsplan: | Schlüsseltyp | Rotationshäufigkeit | Verantwortlich | |———–|———–|———–| | Festplattenverschlüsselungsschlüssel | [TODO: Jährlich] | IT Security | | Datenbankverschlüsselungsschlüssel | [TODO: Jährlich] | Database Admin | | TLS-Zertifikate |

[TODO: Jährlich oder gemäß Anbieter] | IT Security | | VPN-Schlüssel | [TODO: Vierteljährlich] | Network Admin |

11.6 6. Zugriffskontrolllisten (ACLs)

11.6.1 6.1 ACL-Verwaltung

ACL-Prinzipien: - Geringste Privilegien - Need-to-know - Aufgabentrennung - Defense in Depth

ACL-Komponenten: - Benutzer-/Gruppenidentität - Ressource (Datei, Ordner, Anwendung, Datenbank) - Berechtigungen (Lesen, Schreiben, Ausführen, Löschen) - Bedingungen (Zeit, Standort, Gerät)

11.6.2 6.2 Berechtigungsstufen

Standard-Berechtigungsstufen: | Stufe | Beschreibung | Typische Rollen | |——-|————|——————| | Kein Zugriff | Keine Berechtigungen | Standard für alle Benutzer | | Lesen | Nur Ansicht | Auditoren, Nur-Lese-Benutzer | | Lesen/Schreiben | Ansicht und Änderung | Standardbenutzer | | Vollzugriff | Alle Berechtigungen | Administratoren, Eigentümer |

11.6.3 6.3 ACL-Überprüfung

Überprüfungsprozess: - **Häufigkeit:** Vierteljährlich - **Umfang:** Alle ePHI-Ressourcen - **Prüfer:** Ressourceneigentümer + Security Officer - **Maßnahmen:** Unnötige Berechtigungen entfernen, für Rollenänderungen aktualisieren

11.7 7. Privileged Access Management (PAM)

11.7.1 7.1 Definition privilegierter Konten

Privilegierte Konten: - Systemadministratoren - Datenbankadministratoren - Netzwerkadministratoren - Anwendungsadministratoren - Sicherheitsadministratoren

Eigenschaften privilegierten Zugriffs: - Erhöhte Berechtigungen - Zugriff auf sensible Systeme - Fähigkeit zur Änderung von Sicherheitskontrollen - Zugriff auf alle ePHI

11.7.2 7.2 PAM-Kontrollen

PAM-Anforderungen: - Trennung privilegierter Konten von Standardkonten - Just-in-Time (JIT) Privilegienerweiterung - Sitzungsaufzeichnung für privilegierten Zugriff - Erweiterte Überwachung und Alarmierung - Regelmäßige Zugriffsüberprüfungen - MFA für privilegierten Zugriff erforderlich

PAM-Lösung: [TODO: CyberArk, BeyondTrust, Thycotic usw.]

11.8 8. Überwachung und Auditing

11.8.1 8.1 Zugriffsüberwachung

Überwachungsaktivitäten: - Fehlgeschlagene Anmeldeversuche - Erfolgreiche Anmeldungen (insbesondere außerhalb der Geschäftszeiten) - Nutzung privilegierter Konten - Nutzung von Notfallzugang - Berechtigungsänderungen - Kontoerstellung/-löschung - Passwortzurücksetzungen

Überwachungstools: - SIEM (Security Information and Event Management) - Log-Aggregation und -Analyse - User Behavior Analytics (UBA) - Automatisierte Alarmierung

11.8.2 8.2 Zugriffs-Auditing

Audit-Aktivitäten: - Benutzerzugriffsüberprüfungen - Privilegierte Zugriffsüberprüfungen - ACL-Überprüfungen - Inaktive Kontoüberprüfungen - Verwaiste Kontoüberprüfungen

Audit-Häufigkeit: | Aktivität | Häufigkeit | Verantwortlich | |————|————|————-| | Benutzerzugriffsüberprüfung | Vierteljährlich | Manager + Security Officer | | Privilegierte Zugriffsüberprüfung | Monatlich | Security Officer | | ACL-Überprüfung | Vierteljährlich | Ressourceneigentümer | | Inaktive Kontoüberprüfung | Monatlich | IT + HR |

11.9 9. Dokumentation und Aufzeichnungen

11.9.1 9.1 Erforderliche Dokumentation

- Benutzerkontoinventar
- Privilegiertes Kontoinventar
- Break-Glass-Kontoverfahren
- Notfallzugriffsprotokolle
- Zugriffsüberprüfungsaufzeichnungen
- ACL-Dokumentation
- Verschlüsselungsschlüsselinventar
- Timeout-Konfigurationsdokumentation

11.9.2 9.2 Aufbewahrung

Aufbewahrungsfrist: [TODO: 6 Jahre ab Erstellung oder letztem Gültigkeitsdatum]

Speicherort: [TODO: Identitätsverwaltungssystem, Dokumenten-Repository]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 12

Datenschutzpraktiken und Individuelle Rechte

Dokument-ID: HIPAA-0500
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

12.1 1. Zweck

Dieses Dokument beschreibt die Datenschutzpraktiken und Verfahren zur Verwaltung individueller Rechte gemäß der HIPAA Privacy Rule für AdminSend GmbH.

12.1.1 1.1 HIPAA-Anforderungen

Privacy Rule-Anforderungen: - Datenschutzerklärung (§164.520) - Zugriffsrecht (§164.524) - Recht auf Änderung (§164.526) - Rechenschaftspflicht für Offenlegungen (§164.528) - Recht auf Einschränkungsanfragen (§164.522(a)) - Recht auf vertrauliche Kommunikation (§164.522(b))

12.2 2. Datenschutzerklärung

12.2.1 2.1 Anforderungen an die Erklärung

Inhaltsanforderungen: - Verwendungen und Offenlegungen von PHI - Individuelle Rechte - Pflichten der Covered Entity - Beschwerdeverfahren - Kontaktinformationen - Gültigkeitsdatum

Verteilung: - Bei erster Leistungserbringung - Auf Anfrage - Gut sichtbar ausgehängt - Auf Website verfügbar - Wesentliche Änderungen erfordern neue Erklärung

12.2.2 2.2 Erforderliche Inhalte der Datenschutzerklärung

Kopfzeile: - Titel: “DATENSCHUTZERKLÄRUNG” - Gültigkeitsdatum - Organisationsname

Abschnitt 1: Verwendungen und Offenlegungen

Zulässige Verwendungen ohne Autorisierung: - Behandlung - Zahlung - Gesundheitsoperationen - Gesetzlich vorgeschrieben - Öffentliche Gesundheitsaktivitäten - Missbrauch, Vernachlässigung oder häusliche Gewalt - Gesundheitsaufsichtsaktivitäten - Gerichtsverfahren - Strafverfolgung - Gerichtsmediziner, Bestatter - Organ-/Gewebespende - Forschung (begrenzt) - Ernsthafte Bedrohung - Wesentliche Regierungsfunktionen - Workers' Compensation

Verwendungen, die Autorisierung erfordern: - Marketing - Verkauf von PHI - Psychotherapienotizen (meistens) - Andere nicht aufgeführte Zwecke

Abschnitt 2: Ihre Rechte bezüglich Ihrer Gesundheitsinformationen

Die Erklärung muss folgende Rechte beschreiben: 1. Recht auf Zugriff auf Ihre Gesundheitsinformationen 2. Recht auf Änderung Ihrer Gesundheitsinformationen 3. Recht auf Rechenschaftspflicht für Offenlegungen 4. Recht auf Einschränkungsanfragen 5. Recht auf vertrauliche Kommunikation 6. Recht auf eine Kopie dieser Datenschutzerklärung 7. Recht auf Beschwerde

Abschnitt 3: Unsere Pflichten - Privatsphäre Ihrer Gesundheitsinformationen wahren - Ihnen diese Datenschutzerklärung zur Verfügung stellen - Den in dieser Erklärung beschriebenen Bedingungen folgen - Sie über Datenschutzverletzungen benachrichtigen

12.2.3 2.3 Verteilungsverfahren

Erstverteilung: - Bei erster Leistungserbringung an Einzelperson - Spätestens am Datum der ersten Leistungserbringung - Guter Glaube, Erklärung bereitzustellen

Elektronische Verteilung: - Falls elektronische Leistungserbringung - Elektronische Erklärung verfügbar machen - Möglichkeit, Papierkopie anzufordern

Physische Verteilung: - Gut sichtbar in Einrichtung ausgehängt - In Wartebereichen verfügbar - Am Empfang verfügbar

Website-Veröffentlichung: - Auf Organisations-Website veröffentlichen - Prominent platzieren - Leicht zugänglich

Auf Anfrage: - Kopie auf Anfrage innerhalb von [TODO: 7 Tagen] bereitstellen - Keine Gebühr für erste Kopie

12.2.4 2.4 Bestätigung des Erhalts

Bestätigungsanforderungen: - Guter Glaube, schriftliche Bestätigung zu erhalten - Dokumentieren, wenn Bestätigung nicht erhalten - Grund dokumentieren, warum nicht erhalten

Bestätigungsmethoden: - Unterschrift auf Papierformular - Elektronische Bestätigung - E-Mail-Bestätigung

Dokumentation: - Bestätigungen für [TODO: 6 Jahre] aufbewahren - Dokumentieren, wenn Bestätigung abgelehnt - Grund für Nichterhalt dokumentieren

12.2.5 2.5 Überarbeitungen der Datenschutzerklärung

Wann Überarbeitung erforderlich: - Wesentliche Änderung der Verwendungen/Offenlegungen - Änderung der Rechte von Einzelpersonen - Änderung der rechtlichen Pflichten - Änderung anderer Datenschutzpraktiken

Überarbeitungsprozess: 1. **Entwurf:** Neue Erklärung entwerfen 2. **Überprüfung:** Privacy Officer überprüft 3. **Genehmigung:** Rechtsabteilung genehmigt 4. **Gültigkeitsdatum:** Neues Gültigkeitsdatum festlegen 5. **Verteilung:** Neue Erklärung verteilen 6. **Veröffentlichung:** Auf Website veröffentlichen, in Einrichtung aushängen 7. **Verfügbarkeit:** Auf Anfrage verfügbar machen

Benachrichtigung über Änderungen: - Einzelpersonen über wesentliche Änderungen benachrichtigen - Neue Erklärung bei nächstem Besuch bereitstellen - Auf Website veröffentlichen

12.3 3. Recht auf Zugriff (§164.524)

12.3.1 3.1 Zugriffsanforderungen

Umfang des Zugriffsrechts: - Einzelpersonen haben Recht auf Zugriff auf PHI im Designated Record Set - Zugriff auf Kopien oder Einsicht - Zugriff auf elektronische Kopien, falls elektronisch geführt

Designated Record Set: - Medizinische Aufzeichnungen - Abrechnungsaufzeichnungen - Andere Aufzeichnungen, die für Entscheidungen verwendet werden

Ausnahmen vom Zugriffsrecht: - Psychotherapienotizen - Informationen, die für Gerichtsverfahren gesammelt wurden - Informationen, die durch CLIA verboten sind - Informationen von anderen (mit Ausnahmen)

12.3.2 3.2 Zugriffsanfrageprozess

Anfrageverfahren: 1. **Anfrage:** Einzelperson reicht schriftliche Anfrage ein 2. **Überprüfung:** Privacy Officer überprüft Anfrage 3. **Identitätsüberprüfung:** Identität der Person überprüfen 4. **Umfang:** Umfang der angeforderten Informationen bestimmen 5. **Ausnahmen:** Auf Ausnahmen prüfen 6. **Genehmigung:** Zugriff genehmigen oder ablehnen 7. **Bereitstellung:** Kopien bereitstellen oder Einsicht arrangieren 8. **Dokumentation:** Anfrage und Antwort dokumentieren

Anfrageformular: - Name der Person - Kontaktinformationen - Beschreibung der angeforderten Informationen - Zeitraum - Format (Papier, elektronisch) - Zustellungsmethode - Unterschrift und Datum

12.3.3 3.3 Zeitrahmen für Antwort

Standard-Zeitrahmen: - [TODO: 30 Tage] ab Erhalt der Anfrage - Einmalige Verlängerung um [TODO: 30 Tage] zulässig - Schriftliche Benachrichtigung über Verlängerung erforderlich

Beschleunigte Anfragen: - Dringende Anfragen priorisieren - Schnellere Antwort, wenn möglich

12.3.4 3.4 Format und Zustellung

Format: - Format, das von der Person angefordert wird (falls leicht produzierbar) - Elektronisches Format, falls angefordert und elektronisch geführt - Papierformat als Standard

Zustellungsmethoden: - Persönliche Abholung - Post - Sichere E-Mail (falls angefordert) - Elektronisches Portal

Zustellung an Dritte: - Falls von Person angefordert - Schriftliche, unterzeichnete Anfrage erforderlich - Klare Anweisungen zur Zustellung

12.3.5 3.5 Gebühren

Zulässige Gebühren: - Kosten für Kopieren (Arbeit und Materialien) - Kosten für Porto (falls verschickt) - Kosten für Zusammenfassung (falls angefordert)

Verbotene Gebühren: - Kosten für Suche/Abruf - Kosten für Überprüfung - Übermäßige Gebühren

Gebührenstruktur: - [TODO: Gebühr pro Seite für Papier] - [TODO: Gebühr für elektronische Kopien] - [TODO: Portokosten]

12.3.6 3.6 Ablehnung des Zugriffs

Gründe für Ablehnung: - Informationen nicht im Designated Record Set - Ausnahmen gelten - Zugriff würde Schaden verursachen (überprüfbare Ablehnungen)

Überprüfbare Ablehnungen: - Zugriff würde wahrscheinlich Schaden verursachen - Bezieht sich auf andere Person - Anfrage von persönlichem Vertreter, der Schaden verursachen könnte

Ablehnungsprozess: 1. **Überprüfung:** Grund für Ablehnung überprüfen 2. **Dokumentation:** Grund dokumentieren 3. **Benachrichtigung:** Person schriftlich benachrichtigen 4. **Überprüfungsrechte:** Über Überprüfungsrechte informieren (falls zutreffend) 5. **Beschwerdeverfahren:** Über Beschwerdeverfahren informieren

Ablehnungsschreiben muss enthalten: - Grund für Ablehnung - Überprüfungsrechte (falls zutreffend) - Beschwerdeverfahren - Kontaktinformationen für Beschwerden

12.4 4. Recht auf Änderung (§164.526)

12.4.1 4.1 Änderungsanforderungen

Umfang des Änderungsrechts: - Einzelpersonen haben Recht, Änderung von PHI anzufordern - Gilt für Informationen im Designated Record Set - Organisation kann ablehnen, wenn Informationen korrekt sind

Änderung vs. Ergänzung: - Änderung: Korrektur falscher Informationen - Ergänzung: Hinzufügen zusätzlicher Informationen

12.4.2 4.2 Änderungsanfrageprozess

Anfrageverfahren: 1. **Anfrage:** Schriftliche Anfrage mit Begründung 2. **Überprüfung:** Privacy Officer überprüft Anfrage 3. **Bewertung:** Genauigkeit der Informationen bewerten 4. **Entscheidung:** Genehmigen oder ablehnen 5. **Umsetzung:** Änderung vornehmen (falls genehmigt) 6. **Benachrichtigung:** Person und relevante Parteien benachrichtigen 7. **Dokumentation:** Anfrage und Entscheidung dokumentieren

Anfrageformular: - Name der Person - Beschreibung der zu ändernden Informationen - Vorgeschlagene Änderung - Begründung für Änderung - Unterschrift und Datum

12.4.3 4.3 Zeitrahmen für Antwort

Standard-Zeitrahmen: - [TODO: 60 Tage] ab Erhalt der Anfrage - Einmalige Verlängerung um [TODO: 30 Tage] zulässig - Schriftliche Benachrichtigung über Verlängerung erforderlich

12.4.4 4.4 Genehmigung der Änderung

Wenn genehmigt: 1. **Änderung vornehmen:** Aufzeichnung ändern 2. **Kennzeichnung:** Änderung kennzeichnen 3. **Original beibehalten:** Original nicht löschen 4. **Benachrichtigung:** Person benachrichtigen 5. **Relevante Parteien:** Andere benachrichtigen, die Informationen haben 6. **Zukünftige Offenlegungen:** Änderung in zukünftige Offenlegungen einbeziehen

Benachrichtigung relevanter Parteien: - Personen, die von Person identifiziert wurden - Personen, von denen bekannt ist, dass sie Informationen haben - Personen, die Informationen für Versorgung benötigen

12.4.5 4.5 Ablehnung der Änderung

Gründe für Ablehnung: - Informationen nicht von Organisation erstellt - Informationen nicht im Designated Record Set - Informationen nicht für Einsicht verfügbar - Informationen sind korrekt und vollständig

Ablehnungsprozess: 1. **Benachrichtigung:** Person schriftlich benachrichtigen 2. **Grund:** Grund für Ablehnung angeben 3. **Widerspruchsrecht:** Über Recht auf Widerspruch informieren 4. **Widerspruchsverfahren:** Verfahren zur Einreichung eines Widerspruchs beschreiben 5. **Beschwerdeverfahren:** Über Beschwerdeverfahren informieren

Widerspruch der Person: - Person kann schriftlichen Widerspruch einreichen - Organisation kann Erwiderung vorbereiten - Widerspruch und Erwiderung mit Aufzeichnung aufbewahren - Widerspruch in zukünftige Offenlegungen einbeziehen

12.5 5. Rechenschaftspflicht für Offenlegungen (§164.528)

12.5.1 5.1 Anforderungen an Rechenschaftspflicht

Umfang: - Einzelpersonen haben Recht auf Rechenschaftspflicht für Offenlegungen - Gilt für Offenlegungen in den letzten 6 Jahren - Bestimmte Offenlegungen ausgenommen

Ausnahmen von Rechenschaftspflicht: - Offenlegungen für Behandlung, Zahlung, Gesundheitsoperationen - Offenlegungen an die Person - Offenlegungen gemäß Autorisierung - Offenlegungen für Einrichtungsverzeichnis - Offenlegungen an Personen, die an Versorgung beteiligt sind - Offenlegungen für nationale Sicherheit - Offenlegungen an Strafverfolgungsbehörden (bestimmte) - Offenlegungen vor Compliance-Datum

12.5.2 5.2 Rechenschaftspflichtprotokoll

Erforderliche Informationen: - Datum der Offenlegung - Name und Adresse des Empfängers - Kurze Beschreibung der offengelegten Informationen - Kurze Erklärung des Zwecks der Offenlegung

Protokollierungssystem: - Zentralisiertes Protokollierungssystem - Elektronisches Tracking - Leicht durchsuchbar - Sichere Speicherung

Aufbewahrung: - Mindestens 6 Jahre aufbewahren - Länger, falls durch staatliches Recht erforderlich

12.5.3 5.3 Rechenschaftspflichtanfrageprozess

Anfrageverfahren: 1. **Anfrage:** Schriftliche oder mündliche Anfrage 2. **Überprüfung:** Privacy Officer überprüft Anfrage 3. **Identitätsüberprüfung:** Identität überprüfen 4. **Zeitraum:** Angeforderten Zeitraum bestimmen 5. **Suche:** Rechenschaftspflichtprotokoll durchsuchen 6. **Zusammenstellung:** Rechenschaftspflichtliste zusammenstellen 7. **Bereitstellung:** Liste bereitstellen 8. **Dokumentation:** Anfrage und Antwort dokumentieren

Zeitrahmen: - [TODO: 60 Tage] ab Erhalt der Anfrage - Einmalige Verlängerung um [TODO: 30 Tage] zulässig

Gebühren: - Erste Rechenschaftspflicht in 12 Monaten: Keine Gebühr - Nachfolgende Rechenschaftspflichten: Angemessene kostenbasierte Gebühr - Person im Voraus über Gebühr informieren

12.5.4 5.4 Format der Rechenschaftspflicht

Rechenschaftspflichtliste muss enthalten: | Datum | Empfänger | Beschreibung | Zweck | |——-|———|————|——-| | [Datum] | [Name und Adresse] | [Kurze Beschreibung] | [Zweck] |

Elektronisches Format: - Falls angefordert - Durchsuchbar - Leicht lesbar

12.6 6. Recht auf Einschränkungsanfragen (§164.522(a))

12.6.1 6.1 Einschränkungsanforderungen

Umfang: - Einzelpersonen können Einschränkungen der Verwendungen/Offenlegungen anfordern - Organisation nicht verpflichtet, zuzustimmen (mit Ausnahmen) - Falls zugestimmt, muss Organisation Einschränkung befolgen

Erforderliche Einschränkungen: - Offenlegung an Krankenversicherung für Zahlung/Gesundheitsoperationen - Wenn Person vollständig aus eigener Tasche bezahlt hat - Offenlegung nicht gesetzlich vorgeschrieben

12.6.2 6.2 Einschränkungsanfrageprozess

Anfrageverfahren: 1. **Anfrage:** Schriftliche Anfrage 2. **Überprüfung:** Privacy Officer überprüft Anfrage 3. **Bewertung:** Machbarkeit bewerten 4. **Entscheidung:** Zustimmen oder ablehnen 5. **Dokumentation:** Entscheidung dokumentieren 6. **Benachrichtigung:** Person benachrichtigen 7. **Umsetzung:** Einschränkung umsetzen (falls zugestimmt)

Anfrageformular: - Name der Person - Beschreibung der angeforderten Einschränkung - Spezifische Informationen einzuschränken - Spezifische Personen/Organisationen - Begründung - Unterschrift und Datum

12.6.3 6.3 Zustimmung zu Einschränkungen

Wenn zugestimmt: - Einschränkung in System dokumentieren - Alle relevanten Mitarbeiter benachrichtigen - Einschränkung in Aufzeichnung kennzeichnen - Einschränkung befolgen (außer in Notfällen)

Notfallausnahme: - Einschränkung kann in Notfällen aufgehoben werden - Nur wenn für Notfallbehandlung erforderlich - Person nach Notfall benachrichtigen

12.6.4 6.4 Beendigung von Einschränkungen

Beendigung durch Person: - Person kann Einschränkung jederzeit beenden - Schriftliche Anfrage empfohlen - Gilt nur für zukünftige Informationen

Beendigung durch Organisation: - Organisation kann Einschränkung beenden - Person im Voraus benachrichtigen - Gilt nur für zukünftige Informationen - Einschränkung für bereits erhaltene Informationen bleibt bestehen

12.7 7. Recht auf vertrauliche Kommunikation (§164.522(b))

12.7.1 7.1 Anforderungen an vertrauliche Kommunikation

Umfang: - Einzelpersonen können alternative Kommunikationsmittel oder -orte anfordern - Organisation muss angemessene Anfragen berücksichtigen - Keine Begründung erforderlich (für Gesundheitsdienstleister)

Beispiele: - Alternative Postanschrift - Alternative Telefonnummer - Sichere E-Mail - Persönliche Abholung

12.7.2 7.2 Anfrageprozess

Anfrageverfahren: 1. **Anfrage:** Schriftliche oder mündliche Anfrage 2. **Überprüfung:** Privacy Officer überprüft Anfrage 3. **Bewertung:** Angemessenheit bewerten 4. **Genehmigung:** Angemessene Anfragen genehmigen 5. **Umsetzung:** Alternative Kommunikation umsetzen 6. **Dokumentation:** Anfrage und Genehmigung dokumentieren 7. **Systemaktualisierung:** Kommunikationspräferenzen aktualisieren

Anfrageformular: - Name der Person - Alternative Kontaktmethode - Alternative Adresse/Telefonnummer - Unterschrift und Datum

12.7.3 7.3 Angemessenheitsbewertung

Angemessene Anfragen: - Praktisch umsetzbar - Keine übermäßige Belastung - Keine Beeinträchtigung der Versorgungsqualität

Unangemessene Anfragen: - Technisch nicht machbar - Übermäßige Kosten - Beeinträchtigung der Versorgung

12.7.4 7.4 Umsetzung

Systemaktualisierungen: - Präferenzen in EHR dokumentieren - Abrechnungssystem aktualisieren - Alle relevanten Systeme aktualisieren - Mitarbeiter benachrichtigen

Laufende Compliance: - Präferenzen bei jeder Kommunikation überprüfen - Alternative Methoden verwenden - Regelmäßig mit Person bestätigen

12.8 8. Beschwerdeverfahren

12.8.1 8.1 Beschwerderechte

Recht auf Beschwerde: - Einzelpersonen können sich über Datenschutzpraktiken beschweren - Keine Vergeltungsmaßnahmen erlaubt - Beschwerden intern oder bei HHS

Beschwerdegründe: - Verletzung der Datenschutzrechte - Nichteinhaltung der Datenschutzerklärung - Unbefugte Offenlegung - Verweigerung des Zugriffs - Andere Datenschutzbedenken

12.8.2 8.2 Internes Beschwerdeverfahren

Beschwerdeprozess: 1. **Einreichung:** Beschwerde schriftlich oder mündlich einreichen 2. **Empfang:** Privacy Officer erhält Beschwerde 3. **Dokumentation:** Beschwerde dokumentieren 4. **Untersuchung:** Beschwerde untersuchen 5. **Lösung:** Beschwerde lösen 6. **Antwort:** Person antworten 7. **Nachverfolgung:** Nachverfolgung sicherstellen

Kontaktinformationen: - Privacy Officer: {{ meta.roles.privacy_officer.name }} - E-Mail: {{ meta.roles.privacy_officer.email }} - Telefon: [TODO: Telefonnummer] - Adresse: [TODO: Postanschrift]

Zeitrahmen: - Beschwerde innerhalb von [TODO: 30 Tagen] bestätigen - Untersuchung innerhalb von [TODO: 60 Tagen] abschließen - Person über Ergebnis informieren

12.8.3 8.3 HHS-Beschwerden

Einreichung bei HHS: - Beschwerden können bei HHS Office for Civil Rights eingereicht werden - Innerhalb von 180 Tagen nach Vorfall - Schriftlich per Post oder online

HHS-Kontaktinformationen: - Office for Civil Rights - U.S. Department of Health and Human Services - Online: https://www.hhs.gov/ocr/privacy/hipaa/complaints/

12.8.4 8.4 Keine Vergeltungsmaßnahmen

Verbotene Vergeltungsmaßnahmen: - Keine Vergeltung für Beschwerdeeinreichung - Keine Vergeltung für Ausübung von Rechten - Keine Einschüchterung oder Belästigung

Vergeltungsschutz: - In Datenschutzerklärung dokumentiert - Mitarbeiter geschult - Vergeltungsvorwürfe untersucht - Disziplinarmaßnahmen bei Vergeltung

12.9 9. Schulung und Sensibilisierung

12.9.1 9.1 Schulungsanforderungen

Mitarbeiterschulung: - Datenschutzrechte von Einzelpersonen - Verfahren zur Bearbeitung von Anfragen - Zeitrahmen und Anforderungen - Dokumentation - Keine Vergeltungsmaßnahmen

Häufigkeit: - Erstschulung bei Einstellung - Jährliche Auffrischung - Bei Richtlinienänderungen

12.9.2 9.2 Patientenaufklärung

Aufklärungsmaterialien: - Broschüren über Datenschutzrechte - Poster in Einrichtung - Website-Informationen - Häufig gestellte Fragen

Aufklärungsthemen: - Wie man auf Aufzeichnungen zugreift - Wie man Änderungen anfordert - Wie man Rechenschaftspflicht anfordert - Wie man Beschwerde einreicht

12.10 10. Dokumentation und Aufzeichnungen

12.10.1 10.1 Erforderliche Dokumentation

- Datenschutzerklärung (aktuelle und frühere Versionen)
- Bestätigungen des Erhalts
- Zugriffsanfragen und -antworten
- Änderungsanfragen und -entscheidungen
- Rechenschaftspflichtanfragen und -listen
- Einschränkungsanfragen und -vereinbarungen
- Anfragen zu vertraulicher Kommunikation
- Beschwerden und Lösungen
- Schulungsunterlagen

12.10.2 10.2 Aufbewahrung

Aufbewahrungsfrist: [TODO: 6 Jahre ab Erstellung oder letztem Gültigkeitsdatum]

Speicherort: [TODO: Datenschutzverwaltungssystem, Dokumenten-Repository]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 13

Datenschutzverletzungsmeldung und Incident Response

Dokument-ID: HIPAA-0600
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

13.1 1. Zweck

Dieses Dokument beschreibt die Verfahren zur Datenschutzverletzungsmeldung und Incident Response für AdminSend GmbH gemäß der HIPAA Breach Notification Rule.

13.1.1 1.1 HIPAA-Anforderungen

Breach Notification Rule (45 CFR §§ 164.400-164.414): - Definition und Bewertung von Datenschutzverletzungen - Benachrichtigung von Einzelpersonen - Benachrichtigung von HHS - Benachrichtigung der Medien (500+ Einzelpersonen) - Benachrichtigungspflichten von Business Associates

13.2 2. Definition von Datenschutzverletzungen

Datenschutzverletzung: Erwerb, Zugriff, Nutzung oder Offenlegung von PHI auf eine Weise, die nicht gemäß der Privacy Rule zulässig ist und die Sicherheit oder Privatsphäre der PHI gefährdet.

Ausnahmen: - Unbeabsichtigter Erwerb/Zugriff durch Mitarbeiter in gutem Glauben - Versehentliche Offenlegung innerhalb der Organisation - Offenlegung, bei der Empfänger Informationen vernünftigerweise nicht behalten kann

13.2.1 2.1 Risikobewertung bei Datenschutzverletzungen

Risikobewertungsfaktoren: 1. Art und Umfang der beteiligten PHI 2. Unbefugte Person, die PHI verwendet/erhalten hat 3. Ob PHI tatsächlich erworben oder eingesehen wurde 4. Ausmaß, in dem das Risiko gemindert wurde

Risikobewertungsprozess: 1. **Vorfallidentifikation:** Potenziellen Vorfall identifizieren 2. **Vorläufige Bewertung:** Schnelle Bewertung durchführen 3. **Detaillierte Analyse:** Jeden Risikofaktor analysieren 4. **Risikostufe:** Risikostufe bestimmen (niedrig, mittel, hoch) 5. **Datenschutzverletzungsfeststellung:** Feststellen, ob Datenschutzverletzung vorliegt 6. **Dokumentation:** Bewertung dokumentieren 7. **Benachrichtigungsentscheidung:** Benachrichtigungsanforderungen bestimmen

Risikobewertungsmatrix: | Faktor | Niedrig | Mittel | Hoch | |———|———|———|——| | Art der PHI | Demografische Daten | Klinische Daten | Sensible Daten (HIV, psychische Gesundheit) | | Umfang | 1-10 Personen | 11-499 Personen | 500+ Personen | | Empfänger | Autorisiertes Personal | Nicht autorisiertes Personal intern | Externe unbefugte Partei | | Erwerb | Nicht eingesehen | Möglicherweise eingesehen | Definitiv eingesehen/kopiert | | Minderung | Vollständig gemindert | Teilweise gemindert | Nicht gemindert |

13.2.2 2.2 Dokumentation der Risikobewertung

Erforderliche Dokumentation: - Datum und Zeit des Vorfalls - Beschreibung des Vorfalls - Betroffene PHI - Anzahl betroffener Personen - Analyse jedes Risikofaktors - Datenschutzverletzungsfeststellung - Begründung für Feststellung - Benachrichtigungsentscheidung

Aufbewahrung: - Alle Risikobewertungen für [TODO: 6 Jahre] aufbewahren - Auch wenn keine Datenschutzverletzung festgestellt wurde

13.3 3. Benachrichtigung von Einzelpersonen

13.3.1 3.1 Benachrichtigungsanforderungen

Wann Benachrichtigung erforderlich: - Datenschutzverletzung festgestellt - Ungesicherte PHI betroffen - Mehr als niedriges Risiko für Einzelperson

Zeitrahmen: - Ohne unangemessene Verzögerung - Spätestens [TODO: 60 Tage] nach Entdeckung - Früher, wenn möglich

Benachrichtigungsmethode: - **Erste Priorität:** Schriftliche Benachrichtigung per Post - **Alternative:** E-Mail (falls Person zugestimmt hat) - **Ersatz:** Wenn Kontaktinformationen unzureichend

13.3.2 3.2 Inhalt der Benachrichtigung an Einzelpersonen

Erforderliche Elemente: 1. **Beschreibung:** Kurze Beschreibung der Datenschutzverletzung 2. **Betroffene PHI:** Arten von PHI betroffen 3. **Schritte der Person:** Schritte, die Person unternehmen sollte 4. **Maßnahmen der Organisation:** Schritte zur Untersuchung und Minderung 5. **Kontaktinformationen:** Kontakt für weitere Informationen 6. **Datum:** Datum der Datenschutzverletzung (falls bekannt)

Klare Sprache: - Einfache, nicht-technische Sprache - Auf Deutsch (oder bevorzugter Sprache) - Leicht verständlich - Keine Rechtfertigungen oder Schuldzuweisungen

Beispielbenachrichtigung:

```
Betreff: Wichtige Benachrichtigung über Ihre Gesundheitsinformationen

Sehr geehrte/r [Name],

Wir schreiben Ihnen, um Sie über einen Vorfall zu informieren, der Ihre
geschützten Gesundheitsinformationen (PHI) betreffen könnte.

Was ist passiert:
[Beschreibung des Vorfalls]

Welche Informationen waren betroffen:
[Arten von PHI]

Was wir tun:
[Maßnahmen der Organisation]

Was Sie tun sollten:
[Empfohlene Schritte]

Für weitere Informationen:
[Kontaktinformationen]

Mit freundlichen Grüßen,
[Organisation]
```

13.3.3 3.3 Benachrichtigungsmethoden

Schriftliche Benachrichtigung (Standard): - Per Post an letzte bekannte Adresse - Erstklassige Post - Einzeln adressiert

E-Mail-Benachrichtigung: - Nur wenn Person zugestimmt hat - Sichere E-Mail bevorzugt - Lesebestätigung anfordern

Ersatzbenachrichtigung: - Wenn Kontaktinformationen unzureichend für < 10 Personen: - Alternative schriftliche Benachrichtigung - Telefonische Benachrichtigung - Andere verfügbare Mittel

- Wenn Kontaktinformationen unzureichend für 10 Personen:
  - Auffällige Veröffentlichung auf Website für 90 Tage
  - Benachrichtigung in großen Medien (Zeitung, Radio)

Dringende Benachrichtigung: - Telefonische Benachrichtigung zusätzlich zu schriftlicher - Wenn sofortige Maßnahmen erforderlich - Dokumentieren Sie Anruf

13.3.4 3.4 Dokumentation der Benachrichtigung

Erforderliche Aufzeichnungen: - Liste aller benachrichtigten Personen - Datum der Benachrichtigung - Benachrichtigungsmethode - Kopie der Benachrichtigung - Rücklaufpost (unzustellbar) - Ersatzbenachrichtigungsmaßnahmen

13.4 4. Benachrichtigung von HHS

13.4.1 4.1 HHS-Benachrichtigungsanforderungen

Datenschutzverletzungen mit 500+ Personen: - Benachrichtigung an HHS gleichzeitig mit Einzelpersonen - Spätestens 60 Tage nach Entdeckung - Über HHS-Website einreichen

Datenschutzverletzungen mit < 500 Personen: - Jährliche Benachrichtigung an HHS - Innerhalb von 60 Tagen nach Jahresende - Über HHS-Website einreichen

HHS-Einreichungsportal: - https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf - Elektronische Einreichung erforderlich - Bestätigung aufbewahren

13.4.2 4.2 Inhalt der HHS-Benachrichtigung

Erforderliche Informationen: - Name der Organisation - Kontaktinformationen - Datum der Datenschutzverletzung - Datum der Entdeckung - Anzahl betroffener Personen - Beschreibung der Datenschutzverletzung - Arten betroffener PHI - Kurze Beschreibung der Untersuchung - Minderungsmaßnahmen - Korrekturmaßnahmen

Zusätzliche Informationen: - Business Associate beteiligt (falls zutreffend) - Strafverfolgung beteiligt (falls zutreffend) - Medienbenachrichtigung erfolgt (falls zutreffend)

13.4.3 4.3 HHS Breach Portal

Öffentliche Veröffentlichung: - HHS veröffentlicht Datenschutzverletzungen mit 500+ Personen - "Wall of Shame" - Öffentlich durchsuchbar - Bleibt für 24 Monate online

Informationen im Portal: - Name der Organisation - Bundesstaat - Anzahl betroffener Personen - Art der Datenschutzverletzung - Ort der Datenschutzverletzung - Datum der Datenschutzverletzung

13.5 5. Medienbenachrichtigung

13.5.1 5.1 Medienbenachrichtigungsanforderungen

Wann erforderlich: - Datenschutzverletzung betrifft 500+ Personen in einem Bundesstaat/Gerichtsbarkeit - Gleichzeitig mit Benachrichtigung von Einzelpersonen - Spätestens 60 Tage nach Entdeckung

Medienauswahl: - Prominente Medien im betroffenen Bundesstaat/Gebiet - Zeitungen, Fernsehen, Radio - Breite Reichweite

13.5.2 5.2 Inhalt der Medienbenachrichtigung

Erforderliche Informationen: - Ähnlich wie Benachrichtigung an Einzelpersonen - Beschreibung der Datenschutzverletzung - Arten betroffener PHI - Schritte, die Personen unternehmen sollten - Kontaktinformationen für weitere Informationen

Pressemitteilung: - Professionell verfasst - Faktenbasiert - Keine Spekulationen - Kontaktinformationen für Medienanfragen

13.5.3 5.3 Medienmanagement

Medienstrategie: - Sprecher benennen - Konsistente Botschaft - Fakten bereitstellen - Keine Spekulationen - Mitgefühl zeigen

Medienanfragen: - An Sprecher weiterleiten - Konsistente Antworten - Dokumentieren Sie Anfragen - Keine unbefugten Aussagen

13.6 6. Business Associate-Benachrichtigung

13.6.1 6.1 Business Associate-Pflichten

Wenn Business Associate Datenschutzverletzung entdeckt: - Covered Entity ohne unangemessene Verzögerung benachrichtigen - Spätestens 60 Tage nach Entdeckung - Erforderliche Informationen bereitstellen

Benachrichtigungsinhalt: - Beschreibung der Datenschutzverletzung - Betroffene PHI - Anzahl betroffener Personen - Datum der Datenschutzverletzung - Datum der Entdeckung - Untersuchungsergebnisse - Minderungsmaßnahmen

13.6.2 6.2 Covered Entity-Verantwortlichkeiten

Nach Erhalt der Benachrichtigung von Business Associate: 1. **Überprüfung:** Benachrichtigung überprüfen 2. **Bewertung:** Eigene Risikobewertung durchführen 3. **Benachrichtigung:** Einzelpersonen, HHS, Medien benachrichtigen (falls erforderlich) 4. **Dokumentation:** Alle Schritte dokumentieren 5. **Überwachung:** Business Associate-Reaktion überwachen

Business Associate Agreement: - Benachrichtigungspflichten spezifizieren - Zeitrahmen festlegen - Erforderliche Informationen definieren - Kooperationspflichten

13.7 7. Incident Response-Prozess

13.7.1 7.1 Incident Response-Team

Team-Mitglieder: - Privacy Officer (Leiter) - Security Officer - IT-Manager - Rechtsberater - Öffentlichkeitsarbeit/Kommunikation - Betroffene Abteilungsleiter - HR (falls Mitarbeiter beteiligt)

Rollen und Verantwortlichkeiten: | Rolle | Verantwortlichkeiten | |——-|——————| | Privacy Officer | Gesamtleitung, Risikobewertung, Benachrichtigungsentscheidungen | | Security Officer | Technische Untersuchung, Eindämmung, Behebung | | IT-Manager | Systemanalyse, Protokollüberprüfung, technische Unterstützung | | Rechtsberater | Rechtliche Beratung, Compliance-Überprüfung | | Öffentlichkeitsarbeit | Medienmanagement, externe Kommunikation | | HR | Mitarbeiteruntersuchungen, Disziplinarmaßnahmen |

13.7.2 7.2 Incident Response-Phasen

Phase 1: Erkennung und Meldung - Vorfall erkannt - An Privacy Officer/Security Officer gemeldet - Erste Dokumentation

Phase 2: Eindämmung - Sofortige Maßnahmen zur Eindämmung - Weiteren Zugriff verhindern - Beweise sichern

Phase 3: Bewertung - Umfang bestimmen - Betroffene PHI identifizieren - Betroffene Personen zählen - Risikobewertung durchführen

Phase 4: Benachrichtigung - Benachrichtigungsentscheidung treffen - Benachrichtigungen vorbereiten - Einzelpersonen benachrichtigen - HHS benachrichtigen (falls erforderlich) - Medien benachrichtigen (falls erforderlich)

Phase 5: Behebung - Ursache beheben - Schwachstellen schließen - Kontrollen verbessern - Richtlinien aktualisieren

Phase 6: Nachbereitung - Incident Review durchführen - Lessons Learned dokumentieren - Verbesserungen umsetzen - Schulung aktualisieren

13.7.3 7.3 Incident Response-Zeitrahmen

Sofort (0-24 Stunden): - Vorfall eindämmen - Incident Response-Team benachrichtigen - Vorläufige Bewertung - Beweise sichern

Kurzfristig (1-7 Tage): - Detaillierte Untersuchung - Risikobewertung abschließen - Datenschutzverletzungsfeststellung - Benachrichtigungsplan entwickeln

Mittelfristig (7-60 Tage): - Benachrichtigungen versenden - HHS benachrichtigen - Medien benachrichtigen (falls erforderlich) - Behebungsmaßnahmen umsetzen

Langfristig (60+ Tage): - Nachbereitung abschließen - Verbesserungen umsetzen - Überwachung fortsetzen - Dokumentation abschließen

13.8 8. Strafverfolgungsausnahme

13.8.1 8.1 Verzögerung der Benachrichtigung

Wenn Strafverfolgung Verzögerung anfordert: - Benachrichtigung kann verzögert werden - Schriftliche Anfrage von Strafverfolgung erforderlich - Spezifizierter Zeitraum - Dokumentieren Sie Anfrage

Verzögerungszeitraum: - Wie von Strafverfolgung angegeben - Normalerweise 30 Tage - Verlängerungen möglich - Benachrichtigung nach Ablauf

13.8.2 8.2 Zusammenarbeit mit Strafverfolgung

Kooperationspflichten: - Informationen bereitstellen - Beweise bewahren - Untersuchung nicht behindern - Vertraulichkeit wahren

Dokumentation: - Alle Interaktionen dokumentieren - Anfragen aufzeichnen - Bereitgestellte Informationen verfolgen - Verzögerungen rechtfertigen

13.9 9. Schulung und Sensibilisierung

13.9.1 9.1 Mitarbeiterschulung

Schulungsthemen: - Datenschutzverletzungsdefinition - Meldepflichten - Incident Response-Verfahren - Benachrichtigungsanforderungen - Dokumentationspflichten

Häufigkeit: - Erstschulung bei Einstellung - Jährliche Auffrischung - Nach Vorfällen - Bei Richtlinienänderungen

13.9.2 9.2 Incident Response-Übungen

Übungstypen: - Tischübungen (Tabletop) - Simulationen - Vollständige Übungen

Häufigkeit: - Mindestens jährlich - Nach größeren Änderungen - Nach tatsächlichen Vorfällen

Übungsdokumentation: - Übungsszenario - Teilnehmer - Beobachtungen - Lessons Learned - Verbesserungsmaßnahmen

13.10 10. Dokumentation und Aufzeichnungen

13.10.1 10.1 Erforderliche Dokumentation

Vorfallaufzeichnungen: - Vorfallbeschreibung - Entdeckungsdatum - Risikobewertung - Datenschutzverletzungsfeststellung - Benachrichtigungsentscheidung - Benachrichtigungsaufzeichnungen - Untersuchungsergebnisse - Behebungsmaßnahmen - Nachbereitungsbericht

Benachrichtigungsaufzeichnungen: - Benachrichtigungen an Einzelpersonen - HHS-Einreichungen - Medienbenachrichtigungen - Business Associate-Benachrichtigungen - Bestätigungen

13.10.2 10.2 Aufbewahrung

Aufbewahrungsfrist: [TODO: 6 Jahre ab Datum des Vorfalls]

Speicherort: [TODO: Incident Management-System, sicheres Repository]

13.10.3 10.3 Berichterstattung

Interne Berichterstattung: - Monatliche Zusammenfassung an Führung - Vierteljährliche Trendanalyse - Jährlicher Bericht

Externe Berichterstattung: - HHS-Benachrichtigungen - Staatliche Meldungen (falls erforderlich) - Versicherungsmeldungen

13.11 11. Kontinuierliche Verbesserung

13.11.1 11.1 Lessons Learned

Nach jedem Vorfall: - Nachbesprechung durchführen - Was gut funktioniert hat - Was verbessert werden kann - Ursachenanalyse - Verbesserungsmaßnahmen

Dokumentation: - Lessons Learned-Bericht - Empfehlungen - Umsetzungsplan - Verantwortlichkeiten

13.11.2 11.2 Prozessverbesserungen

Regelmäßige Überprüfung: - Incident Response-Verfahren - Benachrichtigungsvorlagen - Kontaktlisten - Schulungsmaterialien

Aktualisierungen: - Basierend auf Lessons Learned - Regulatorische Änderungen - Best Practices - Technologieänderungen

---

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 14

Anhang: Risikoanalyse-Vorlage

Dokument-ID: HIPAA-0700
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

14.1 1. Zweck

Dieser Anhang bietet eine Vorlage zur Durchführung einer HIPAA Security Rule-Risikoanalyse gemäß §164.308(a)(1)(ii)(A).

14.2 2. Risikoanalyse-Vorlage

14.2.1 2.1 Umfangsdefinition

ePHI-Inventar: | Datenelement | Format | Speicherort | Zugriffskontrollen | Verschlüsselung | |—————|————|————-|———————|—————| | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

14.2.2 2.2 Bedrohungs- und Schwachstellenbewertung

Bedrohung	Schwachstelle	Wahrscheinlichkeit	Auswirkung	Risikostufe	Minderung
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

14.2.3 2.3 Risikobehandlungsplan

Risiko-ID	Behandlung	Kontrollen	Zeitplan	Verantwortlich	Status
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Ersterstellung

Beispiel-ePHI-Inventar: | Datenelement | Format | Speicherort | Zugriffskontrollen | Verschlüsselung | |—————|———|————-|———————|—————| | Patientendemografie | Elektronisch | EHR-Datenbank | Rollenbasiert, MFA | TDE, AES-256 | | Klinische Notizen | Elektronisch | EHR-Datenbank | Rollenbasiert, MFA | TDE, AES-256 | | Laborergebnisse | Elektronisch | Labor-System | Rollenbasiert | TDE, AES-256 | | Bildgebungsstudien | Elektronisch | PACS | Rollenbasiert | AES-256 | | Abrechnungsdaten | Elektronisch | Abrechnungssystem | Rollenbasiert | TDE, AES-256 |

Systeminventar: | System | Zweck | ePHI-Typ | Standort | Kritikalität | |———|——-|———-|———-|————| | EHR-System | Patientenakten | Alle PHI | Rechenzentrum | Kritisch | | Labor-System | Laborergebnisse | Laborwerte | Rechenzentrum | Hoch | | PACS | Medizinische Bildgebung | Bilder, Berichte | Rechenzentrum | Hoch | | Abrechnungssystem | Abrechnung | Demografische, Abrechnungsdaten | Rechenzentrum | Hoch |

Bedrohungskategorien: 1. **Externe Bedrohungen:** Hacker, Malware, Ransomware 2. **Interne Bedrohungen:** Böswillige Insider, fahrlässige Mitarbeiter 3. **Naturkatastrophen:** Feuer, Überschwemmung, Erdbeben 4. **Technische Ausfälle:** Hardware-Ausfall, Software-Fehler 5. **Menschliches Versagen:** Versehentliche Offenlegung, Konfigurationsfehler

Beispiel-Bedrohungs- und Schwachstellenmatrix: | Bedrohung | Schwachstelle | Wahrscheinlichkeit | Auswirkung | Risikostufe | Minderung | |————|—————|——————-|————|———-|————| | Ransomware-Angriff | Ungepatchte Systeme | Mittel | Hoch | Hoch | Patch-Management, EDR, Backups | | Unbefugter Zugriff | Schwache Passwörter | Hoch | Mittel | Hoch | MFA, Passwortrichtlinie | | Datenverlust | Fehlende Backups | Niedrig | Hoch | Mittel | Backup-Strategie, Tests | | Insider-Bedrohung | Übermäßige Berechtigungen | Mittel | Hoch | Hoch | Least Privilege, Überwachung | | Phishing | Ungeschulte Mitarbeiter | Hoch | Mittel | Hoch | Schulung, E-Mail-Filterung |

Wahrscheinlichkeitsskala: - **Niedrig:** Unwahrscheinlich innerhalb von 3 Jahren - **Mittel:** Möglich innerhalb von 3 Jahren - **Hoch:** Wahrscheinlich innerhalb von 1 Jahr

Auswirkungsskala: - **Niedrig:** Minimale Auswirkung auf Vertraulichkeit, Integrität, Verfügbarkeit - **Mittel:** Moderate Auswirkung, begrenzte PHI-Offenlegung - **Hoch:** Schwerwiegende Auswirkung, umfangreiche PHI-Offenlegung

Risikobehandlungsoptionen: 1. **Mindern:** Kontrollen implementieren, um Risiko zu reduzieren 2. **Übertragen:** Risiko auf Dritte übertragen (Versicherung) 3. **Vermeiden:** Aktivität einstellen, die Risiko verursacht 4. **Akzeptieren:** Risiko akzeptieren (mit Genehmigung)

Beispiel-Risikobehandlungsplan: | Risiko-ID | Risiko | Behandlung | Kontrollen | Zeitplan | Verantwortlich | Status | Kosten | |———|——|———|———|——-|———–|——|——| | R-001 | Ransomware | Mindern | EDR, Backups, Patch-Management | Q1 2024 | IT Security | In Arbeit | €50.000 | | R-002 | Schwache Passwörter | Mindern | MFA, Passwortrichtlinie | Q1 2024 | IT | Abgeschlossen | €10.000 | | R-003 | Datenverlust | Mindern | Backup-Strategie, Offsite-Backups | Q2 2024 | IT | Geplant | €30.000 | | R-004 | Insider-Bedrohung | Mindern | Least Privilege, SIEM, UBA | Q2 2024 | IT Security | Geplant | €40.000 |

14.2.4 2.4 Kontrollbewertung

Bestehende Kontrollen: | Kontroll-ID | Kontrollname | Typ | Implementiert | Effektiv | Lücken | |———-|———–|—|———–|——-|——| | AC-001 | Eindeutige Benutzer-IDs | Technisch | Ja | Ja | Keine | | AC-002 | Multi-Faktor-Authentifizierung | Technisch | Teilweise | Teilweise | Nicht für alle Systeme | | AC-003 | Automatische Abmeldung | Technisch | Ja | Ja | Keine | | PE-001 | Physische Zugangskontrollen | Physisch | Ja | Teilweise | Einige Bereiche ungesichert | | AD-001 | Zugriffsautorisierung | Administrativ | Ja | Teilweise | Inkonsistente Durchsetzung |

14.2.5 2.5 Gap-Analyse

Identifizierte Lücken: | Lücken-ID | Beschreibung | Betroffene Systeme | Risikostufe | Empfohlene Maßnahme | Priorität | |———|———–|———–|——-|———–|——| | G-001 | MFA nicht für alle Systeme | Labor-System, PACS | Hoch | MFA implementieren | Hoch | | G-002 | Ungesicherte physische Bereiche | Lagerräume | Mittel | Zugangskontrollen hinzufügen | Mittel | | G-003 | Inkonsistente Zugriffsautorisierung | Alle Systeme | Hoch | Prozess standardisieren | Hoch | | G-004 | Niedrige Schulungsabschlussrate | Organisation | Mittel | Schulungsprogramm verbessern | Mittel |

14.3 3. Risikoanalyse-Methodik

14.3.1 3.1 Risikoanalyse-Ansatz

Methodik: - **Qualitativ:** Beschreibende Bewertung (Niedrig, Mittel, Hoch) - **Quantitativ:** Numerische Bewertung (z.B. ALE - Annual Loss Expectancy) - **Hybrid:** Kombination aus qualitativ und quantitativ

14.3.2 3.2 Risikoanalyse-Prozess

10-Schritte-Prozess: 1. **Vorbereitung:** Umfang definieren, Team zusammenstellen 2. **Informationssammlung:** ePHI-Inventar, Systeminventar erstellen 3. **Bedrohungsidentifikation:** Externe und interne Bedrohungen identifizieren 4. **Schwachstellenidentifikation:** Technische, physische, administrative Schwachstellen 5. **Kontrollanalyse:** Bestehende Kontrollen bewerten 6. **Wahrscheinlichkeitsbestimmung:** Wahrscheinlichkeit für jede Bedrohung 7. **Auswirkungsanalyse:** Auswirkung auf Vertraulichkeit, Integrität, Verfügbarkeit 8. **Risikobestimmung:** Risikostufe berechnen 9. **Kontrollempfehlungen:** Kontrollen zur Risikominderung empfehlen 10. **Dokumentation:** Risikoanalysebericht erstellen

14.3.3 3.3 Risikoanalyse-Häufigkeit

Regelmäßige Überprüfungen: - Jährlich (Minimum) - Bei wesentlichen Änderungen - Nach Sicherheitsvorfällen - Bei neuen Bedrohungen

14.4 4. Anhänge

14.4.1 4.1 Anhang A: Risikoanalyse-Checkliste

Vorbereitungsphase: - [ ] Umfang definiert - [ ] Team zusammengestellt - [ ] Ressourcen zugewiesen - [ ] Zeitplan erstellt

Informationssammlungsphase: - [ ] ePHI-Inventar erstellt - [ ] Systeminventar erstellt - [ ] Netzwerkdiagramme überprüft - [ ] Richtlinien überprüft - [ ] Interviews durchgeführt

Bewertungsphase: - [ ] Bedrohungen identifiziert - [ ] Schwachstellen identifiziert - [ ] Kontrollen bewertet - [ ] Wahrscheinlichkeit bestimmt - [ ] Auswirkung analysiert - [ ] Risiken berechnet

Berichtsphase: - [ ] Bericht erstellt - [ ] Überprüft - [ ] Genehmigt - [ ] Verteilt

14.4.2 4.2 Anhang B: Glossar

Begriffe: - **ePHI:** Elektronisch geschützte Gesundheitsinformationen - **Bedrohung:** Potenzielle Ursache eines unerwünschten Vorfalls - **Schwachstelle:** Schwäche, die von Bedrohung ausgenutzt werden kann - **Risiko:** Wahrscheinlichkeit, dass Bedrohung Schwachstelle ausnutzt - **Kontrolle:** Schutzmaßnahme zur Risikominderung - **Wahrscheinlichkeit:** Chance, dass Ereignis eintritt - **Auswirkung:** Schaden, wenn Ereignis eintritt - **Risikostufe:** Kombination aus Wahrscheinlichkeit und Auswirkung

ewpage