Contents

Chapter 1

HIPAA Compliance Handbook

Document Metadata

- **Created on:** 2026-02-10
- **Author:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.5
- **Type:** HIPAA Handbook

---

ewpage

Chapter 2

Scope and Applicability

Document ID: HIPAA-0010
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

2.1 1. Purpose

This document defines the scope of HIPAA compliance for AdminSend GmbH and establishes the applicability of HIPAA Security Rule, Privacy Rule, and Breach Notification Rule requirements.

2.1.1 1.1 Objectives

- **Scope Definition:** Clear identification of HIPAA-regulated activities and systems
- **Compliance Framework:** Establish foundation for HIPAA compliance program
- **Role Clarification:** Define organization's role as Covered Entity or Business Associate
- **PHI Identification:** Document all Protected Health Information within scope

2.1.2 1.2 References

- **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**: Final modifications to HIPAA (2013)

2.2 2. Organization Information

2.2.1 2.1 Organization Details

Organization Name: AdminSend GmbH
Address: Musterstraße 123, 80331 München
State: {{ meta.organization.state }}
Country: Deutschland
Website: https://www.adminsend.de
Tax ID (EIN): {{ meta.organization.tax_id }}

2.2.2 2.2 Organization Type

Primary Classification: [TODO: Select one] - [ ] Covered Entity - Healthcare Provider - [ ] Covered Entity - Health Plan - [ ] Covered Entity - Healthcare Clearinghouse - [ ] Business Associate - [ ] Hybrid Entity (both covered and non-covered functions)

If Healthcare Provider: - **Provider Type:** [TODO: Hospital, Clinic, Physician Practice, etc.] - **NPI (National Provider Identifier):** [TODO: 10-digit NPI] - **Specialties:** [TODO: List medical specialties] - **Electronic Transactions:** [TODO: Yes/No - Do you transmit health information electronically?]

If Health Plan: - **Plan Type:** [TODO: Group health plan, Health insurance issuer, HMO, Medicare, Medicaid, etc.] - **Number of Participants:** [TODO: Number] - **Small Health Plan:** [TODO: Yes/No - Fewer than 50 participants]

If Healthcare Clearinghouse: - **Services Provided:** [TODO: Claims processing, billing services, etc.] - **Covered Entities Served:** [TODO: Number and types]

If Business Associate: - **Services Provided:** [TODO: IT services, billing, legal, consulting, etc.] - **Covered Entity Clients:** [TODO: Number] - **Subcontractors:** [TODO: Yes/No]

2.2.3 2.3 Hybrid Entity Designation

Is this a Hybrid Entity? [TODO: Yes/No]

If yes, complete the following:

Healthcare Components (Covered Functions): | Component | Function | Location | PHI Access | |————|———-|———-|————| | [TODO: Department] | [TODO: Function] | [TODO: Location] | [TODO: Yes/No] |

Non-Healthcare Components (Non-Covered Functions): | Component | Function | Location | PHI Access | |————|———-|———-|————| | [TODO: Department] | [TODO: Function] | [TODO: Location] | [TODO: No] |

Designation Documentation: [TODO: Reference to formal hybrid entity designation]

2.3 3. Protected Health Information (PHI)

2.3.1 3.1 PHI Definition

Protected Health Information (PHI) includes individually identifiable health information that is: 1. Created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse 2. Relates to past, present, or future physical or mental health, provision of healthcare, or payment for healthcare 3. Identifies the individual or could be used to identify the individual

2.3.2 3.2 PHI Elements

Demographic Identifiers (18 HIPAA Identifiers): 1. Names 2. Geographic subdivisions smaller than state (street address, city, county, ZIP code) 3. Dates (birth, admission, discharge, death) - except year 4. Telephone numbers 5. Fax numbers 6. Email addresses 7. Social Security numbers 8. Medical record numbers 9. Health plan beneficiary numbers 10. Account numbers 11. Certificate/license numbers 12. Vehicle identifiers and serial numbers 13. Device identifiers and serial numbers 14. Web URLs 15. IP addresses 16. Biometric identifiers (fingerprints, voiceprints) 17. Full-face photographs 18. Any other unique identifying number, characteristic, or code

Health Information: - Medical history and diagnoses - Treatment and procedure information - Medication records - Laboratory and test results - Insurance and billing information - Clinical notes and assessments

2.3.3 3.3 PHI in Organization

Types of PHI Maintained: [TODO: Check all that apply] - [ ] Electronic PHI (ePHI) - stored electronically - [ ] Paper PHI - physical records - [ ] Oral PHI - verbal communications

PHI Data Elements Collected: | Data Element | Format | Storage Location | Retention Period | |————–|——–|——————|——————| | [TODO: Patient demographics] | Electronic | [TODO: EHR system] | [TODO: Years] | | [TODO: Medical records] | Electronic/Paper | [TODO: Location] | [TODO: Years] | | [TODO: Billing information] | Electronic | [TODO: System] | [TODO: Years] | | [TODO: Lab results] | Electronic | [TODO: System] | [TODO: Years] |

2.4 4. Systems and Applications

2.4.1 4.1 Systems Containing PHI

System ID	System Name	Type	PHI Elements	Location	Vendor
[TODO: SYS-001]	[TODO: EHR System]	Application	All PHI	[TODO: On-premise/Cloud]	[TODO: Vendor]
[TODO: SYS-002]	[TODO: Practice Management]	Application	Demographics, Billing	[TODO: Location]	[TODO: Vendor]
[TODO: SYS-003]	[TODO: Lab System]	Application	Lab results	[TODO: Location]	[TODO: Vendor]
[TODO: SYS-004]	[TODO: Imaging System]	Application	Radiology images	[TODO: Location]	[TODO: Vendor]
[TODO: SYS-005]	[TODO: Email System]	Infrastructure	PHI in transit	[TODO: Location]	[TODO: Vendor]

2.4.2 4.2 Infrastructure Components

Component	Type	Function	PHI Access	Location
[TODO: DB-001]	Database Server	PHI storage	Yes	[TODO: Data center]
[TODO: APP-001]	Application Server	PHI processing	Yes	[TODO: Data center]
[TODO: WEB-001]	Web Server	Patient portal	Yes	[TODO: Cloud]
[TODO: FILE-001]	File Server	Document storage	Yes	[TODO: On-premise]
[TODO: BACKUP-001]	Backup System	PHI backup	Yes	[TODO: Location]

2.4.3 4.3 Network Architecture

Network Segments with PHI: - **Clinical Network:** [TODO: Description] - **Administrative Network:** [TODO: Description] - **DMZ:** [TODO: Description] - **Wireless Networks:** [TODO: Description]

Network Diagram: [TODO: Reference to network diagram in diagrams/ folder]

2.5 5. Physical Locations

2.5.1 5.1 Facilities with PHI

Location ID	Facility Name	Address	Type	PHI Present	Staff Count
[TODO: LOC-001]	Main Clinic	[TODO: Address]	Clinical	Yes	[TODO: Number]
[TODO: LOC-002]	Administrative Office	[TODO: Address]	Administrative	Yes	[TODO: Number]
[TODO: LOC-003]	Data Center	[TODO: Address]	IT Infrastructure	Yes	[TODO: Number]
[TODO: LOC-004]	Satellite Clinic	[TODO: Address]	Clinical	Yes	[TODO: Number]

2.5.2 5.2 Remote Access

Remote Access to PHI Allowed: [TODO: Yes/No]

If yes: - **Access Method:** [TODO: VPN, Remote Desktop, Web Portal] - **Authentication:** [TODO: Username/Password, MFA, Smart Card] - **Authorized Users:** [TODO: Roles/Number] - **Devices:** [TODO: Company-owned, BYOD, Both] - **Mobile Device Management:** [TODO: Yes/No, Solution name]

2.6 6. Workforce

2.6.1 6.1 Workforce with PHI Access

Role/Department	Number of Staff	PHI Access Level	Access Justification
[TODO: Physicians]	[TODO: Number]	Full	Direct patient care
[TODO: Nurses]	[TODO: Number]	Full	Direct patient care
[TODO: Medical Assistants]	[TODO: Number]	Limited	Patient intake
[TODO: Billing Staff]	[TODO: Number]	Billing data only	Claims processing
[TODO: IT Staff]	[TODO: Number]	System admin	System maintenance
[TODO: Reception]	[TODO: Number]	Demographics only	Scheduling

2.6.2 6.2 Workforce Training

HIPAA Training Required: Yes (Annual)
Training Topics: - HIPAA Privacy Rule - HIPAA Security Rule - Breach Notification requirements - Organization policies and procedures - Sanctions for violations

Training Records Retention: [TODO: Years]

2.7 7. Business Associates

2.7.1 7.1 Business Associate Relationships

Business Associate	Service Provided	PHI Access	BAA Signed	BAA Date
[TODO: IT Vendor]	IT support	Yes	[TODO: Yes/No]	[TODO: Date]
[TODO: Billing Service]	Medical billing	Yes	[TODO: Yes/No]	[TODO: Date]
[TODO: Cloud Provider]	Data hosting	Yes	[TODO: Yes/No]	[TODO: Date]
[TODO: Shredding Service]	Document destruction	Yes	[TODO: Yes/No]	[TODO: Date]
[TODO: Legal Counsel]	Legal services	Yes	[TODO: Yes/No]	[TODO: Date]

2.7.2 7.2 Subcontractor Relationships

Do Business Associates use Subcontractors? [TODO: Yes/No]

If yes: | Subcontractor | Service | Primary BA | BAA in Place | |————————|————|————————|————————| | [TODO: Name] | [TODO: Service] | [TODO: BA Name] | [TODO: Yes/No] |

2.8 8. Compliance Scope

2.8.1 8.1 Applicable HIPAA Rules

Security Rule (45 CFR Part 164, Subpart C): [TODO: Applicable/Not Applicable] - 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: Applicable/Not Applicable] - 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: Applicable/Not Applicable] - Breach Discovery and Notification (§164.404-§164.410) - Notification by Business Associates (§164.410)

2.8.2 8.2 Exclusions from Scope

Systems/Processes NOT in Scope: | System/Process | Reason for Exclusion | |————————-|————————-| | [TODO: HR System] | No PHI - employee data only | | [TODO: Marketing Database] | De-identified data only | | [TODO: Public Website] | No PHI collected |

2.9 9. Compliance Responsibilities

2.9.1 9.1 Key Roles

Privacy Officer: - **Name:** {{ meta.roles.privacy_officer.name }} - **Email:** {{ meta.roles.privacy_officer.email }} - **Phone:** {{ meta.roles.privacy_officer.phone }}

Security Officer: - **Name:** {{ meta.roles.security_officer.name }} - **Email:** {{ meta.roles.security_officer.email }} - **Phone:** {{ meta.roles.security_officer.phone }}

HIPAA Compliance Officer: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

Contact Person (for individuals exercising rights): - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone] - **Address:** [TODO: Mailing address]

2.9.2 9.2 Governance Structure

HIPAA Compliance Committee: - **Chair:** [TODO: Name, Title] - **Members:** [TODO: List members and titles] - **Meeting Frequency:** [TODO: Monthly/Quarterly] - **Responsibilities:** Oversight of HIPAA compliance program

2.10 10. Scope Changes

2.10.1 10.1 Change Management Process

Triggers for Scope Review: 1. New systems or applications that handle PHI 2. New business associate relationships 3. New physical locations 4. Changes in services provided 5. Organizational restructuring 6. Regulatory changes

Review Process: 1. Identify change 2. Assess HIPAA applicability 3. Update scope documentation 4. Implement required safeguards 5. Update policies and procedures 6. Train affected workforce 7. Document changes

2.10.2 10.2 Scope Review Schedule

Annual Review: [TODO: Month]
Last Review Date: [TODO: Date]
Next Review Date: [TODO: Date]
Reviewed by: [TODO: Name, Title]

2.10.3 10.3 Change History

Date	Change Description	Impact	Approved By
[TODO: Date]	Initial scope definition	N/A	[TODO: Name]
[TODO: Date]	Added new EHR system	Expanded ePHI scope	[TODO: Name]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 3

Covered Entities and Healthcare Components

Document ID: HIPAA-0020
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

3.1 1. Purpose

This document defines AdminSend GmbH's status as a HIPAA Covered Entity and documents all healthcare components and covered functions.

3.1.1 1.1 Objectives

- **Entity Classification:** Clearly define organization's HIPAA status
- **Component Identification:** Document all healthcare components (if hybrid entity)
- **Function Documentation:** List all covered functions and activities
- **Compliance Boundaries:** Establish clear boundaries for HIPAA compliance

3.2 2. Covered Entity Determination

3.2.1 2.1 Covered Entity Definition

Under HIPAA, a Covered Entity is: 1. **Healthcare Provider** that conducts certain transactions electronically 2. **Health Plan** that provides or pays for medical care 3. **Healthcare Clearinghouse** that processes health information

3.2.2 2.2 Organization Classification

AdminSend GmbH is a: [TODO: Select one]

- ☐ **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))

Classification Justification: [TODO: Explain why organization meets covered entity definition]

3.3 3. Healthcare Provider Details

Complete this section if organization is a Healthcare Provider

3.3.1 3.1 Provider Information

Provider Type: [TODO: Select applicable] - [ ] Hospital - [ ] Physician Practice - [ ] Clinic - [ ] Nursing Home - [ ] Pharmacy - [ ] Laboratory - [ ] Ambulance Service - [ ] Other: [TODO: Specify]

National Provider Identifier (NPI): - **NPI Number:** [TODO: 10-digit NPI] - **NPI Type:** [TODO: Type 1 (Individual) or Type 2 (Organization)] - **Enumeration Date:** [TODO: Date]

Medical Specialties: | Specialty | Taxonomy Code | Providers | |————|————|————| | [TODO: Primary Care] | [TODO: Code] | [TODO: Number] | | [TODO: Specialty 1] | [TODO: Code] | [TODO: Number] | | [TODO: Specialty 2] | [TODO: Code] | [TODO: Number] |

3.3.2 3.2 Electronic Transactions

Does the organization transmit health information electronically in connection with a HIPAA standard transaction? [TODO: Yes/No]

HIPAA Standard Transactions Conducted: - [ ] Healthcare claims or equivalent encounter information (837) - [ ] Eligibility for a health plan (270/271) - [ ] Referral certification and authorization (278) - [ ] Healthcare claim status (276/277) - [ ] Enrollment and disenrollment in a health plan (834) - [ ] Healthcare payment and remittance advice (835) - [ ] Health plan premium payments (820) - [ ] Coordination of benefits (837)

Transaction Volume (Annual): | Transaction Type | Volume | Primary Trading Partner | |————————|——|————————-| | [TODO: Claims] | [TODO: Number] | [TODO: Payer name] | | [TODO: Eligibility] | [TODO: Number] | [TODO: Payer name] |

3.3.3 3.3 Healthcare Services Provided

Services Offered: | Service | Description | Location | PHI Generated | |————|————-|————-|————| | [TODO: Primary Care] | [TODO: Description] | [TODO: Location] | Yes | | [TODO: Diagnostic Services] | [TODO: Description] | [TODO: Location] | Yes | | [TODO: Treatment Services] | [TODO: Description] | [TODO: Location] | Yes |

3.4 4. Health Plan Details

Complete this section if organization is a Health Plan

3.4.1 4.1 Health Plan Information

Plan Type: [TODO: Select applicable] - [ ] Group Health Plan - [ ] Health Insurance Issuer - [ ] HMO (Health Maintenance Organization) - [ ] Medicare - [ ] Medicaid - [ ] Medicare Advantage - [ ] Medicare Part D - [ ] TRICARE - [ ] Other: [TODO: Specify]

Plan Characteristics: - **Number of Participants:** [TODO: Number] - **Small Health Plan:** [TODO: Yes/No - Fewer than 50 participants] - **Self-Insured:** [TODO: Yes/No] - **Fully Insured:** [TODO: Yes/No]

Plan Sponsor Information: - **Sponsor Name:** [TODO: Name] - **Sponsor Type:** [TODO: Employer, Union, etc.] - **Relationship to Plan:** [TODO: Description]

3.4.2 4.2 Health Plan Functions

Functions Performed: - [ ] Claims adjudication - [ ] Eligibility determination - [ ] Enrollment and disenrollment - [ ] Premium collection - [ ] Provider network management - [ ] Utilization review - [ ] Case management - [ ] Disease management

PHI Used for: - [ ] Payment - [ ] Healthcare operations - [ ] Treatment coordination - [ ] Quality improvement - [ ] Fraud detection

3.5 5. Healthcare Clearinghouse Details

Complete this section if organization is a Healthcare Clearinghouse

3.5.1 5.1 Clearinghouse Information

Services Provided: - [ ] Claims processing - [ ] Claims scrubbing - [ ] Format conversion - [ ] Transaction routing - [ ] Eligibility verification - [ ] Other: [TODO: Specify]

Covered Entities Served: - **Number of Providers:** [TODO: Number] - **Number of Payers:** [TODO: Number] - **Transaction Volume (Monthly):** [TODO: Number]

Standard Formats Supported: | Transaction | Format | Version | |————————-|———|———| | [TODO: Claims] | X12 837 | [TODO: 5010] | | [TODO: Eligibility] | X12 270/271 | [TODO: 5010] |

3.6 6. Hybrid Entity Designation

Complete this section if organization is a Hybrid Entity

3.6.1 6.1 Hybrid Entity Definition

A Hybrid Entity is an organization that: 1. Performs both covered and non-covered functions 2. Has formally designated its healthcare components 3. Applies HIPAA only to designated healthcare components

Is AdminSend GmbH a Hybrid Entity? [TODO: Yes/No]

3.6.2 6.2 Healthcare Components

Designated Healthcare Components:

Component ID	Component Name	Function	Location	Staff Count
[TODO: HC-001]	[TODO: Medical Clinic]	Healthcare Provider	[TODO: Building A]	[TODO: 25]
[TODO: HC-002]	[TODO: Employee Health Plan]	Health Plan	[TODO: HR Dept]	[TODO: 5]
[TODO: HC-003]	[TODO: Occupational Health]	Healthcare Provider	[TODO: Building B]	[TODO: 10]

Healthcare Component Functions: | Component | Covered Functions | PHI Created/Maintained | |————|————————-|————————| | [TODO: Medical Clinic] | Patient care, billing | Patient records, billing data | | [TODO: Employee Health Plan] | Claims processing | Claims, enrollment data |

3.6.3 6.3 Non-Healthcare Components

Non-Covered Components:

Component ID	Component Name	Function	PHI Access
[TODO: NC-001]	[TODO: Manufacturing]	Product manufacturing	No
[TODO: NC-002]	[TODO: Sales]	Product sales	No
[TODO: NC-003]	[TODO: Corporate IT]	IT support (non-healthcare)	No

Justification for Non-Covered Status: [TODO: Explain why these components are not covered functions]

3.6.4 6.4 Hybrid Entity Documentation

Formal Designation Document: - **Document Title:** [TODO: "Hybrid Entity Designation"] - **Date of Designation:** [TODO: Date] - **Approved by:** [TODO: Board of Directors, CEO, etc.] - **Document Location:** [TODO: File path or reference]

Designation Criteria: - Clear separation of covered and non-covered functions - Separate management and operations - Distinct workforce assignments - Separate physical locations (if applicable)

3.6.5 6.5 Workforce Assignment

Healthcare Component Workforce: | Employee ID | Name | Role | Component | PHI Access | |————-|——|——|————|————| | [TODO: EMP-001] | [TODO: Name] | [TODO: Physician] | HC-001 | Full | | [TODO: EMP-002] | [TODO: Name] | [TODO: Nurse] | HC-001 | Full | | [TODO: EMP-003] | [TODO: Name] | [TODO: Claims Processor] | HC-002 | Limited |

Shared Workforce: | Employee ID | Name | Role | Access to Healthcare Components | |————-|——|——|————————–| | [TODO: EMP-100] | [TODO: Name] | [TODO: IT Support] | HC-001, HC-002 (system admin only) | | [TODO: EMP-101] | [TODO: Name] | [TODO: Legal] | All components (as needed) |

Workforce Training: - Healthcare component workforce: Full HIPAA training - Shared workforce: HIPAA training for healthcare component access - Non-healthcare workforce: No HIPAA training required (unless accessing PHI)

3.7 7. Covered Functions

3.7.1 7.1 Healthcare Operations

Healthcare Operations Performed: - [ ] Quality assessment and improvement - [ ] Case management and care coordination - [ ] Reviewing competence of healthcare professionals - [ ] Underwriting and premium rating (health plans) - [ ] Medical review and utilization review - [ ] Fraud and abuse detection - [ ] Business planning and development - [ ] Business management and general administrative activities

PHI Used for Healthcare Operations: | Operation | PHI Elements Used | Frequency | Responsible Department | |————|————–-|————|——————–| | [TODO: Quality improvement] | [TODO: Clinical data] | [TODO: Quarterly] | [TODO: Quality Dept] | | [TODO: Utilization review] | [TODO: Claims data] | [TODO: Ongoing] | [TODO: UM Dept] |

3.7.2 7.2 Treatment Activities

Treatment Functions: - [ ] Provision of healthcare services - [ ] Coordination of care - [ ] Referral of patients - [ ] Consultation between providers - [ ] Case management

Treatment Locations: | Location | Services | Providers | Patient Volume | |———-|———-|———-|————-| | [TODO: Main Clinic] | [TODO: Primary care] | [TODO: 5 physicians] | [TODO: 100/day] | | [TODO: Satellite Office] | [TODO: Specialty care] | [TODO: 2 specialists] | [TODO: 30/day] |

3.7.3 7.3 Payment Activities

Payment Functions: - [ ] Billing and claims management - [ ] Claims adjudication - [ ] Payment collection - [ ] Reimbursement - [ ] Utilization review for payment - [ ] Pre-authorization

Payment Systems: | System | Function | PHI Processed | Volume | |——|———-|————|——| | [TODO: Billing System] | Claims generation | Billing data | [TODO: 500/day] | | [TODO: Payment Portal] | Patient payments | Demographics, account | [TODO: 100/day] |

3.8 8. Compliance Implications

3.8.1 8.1 HIPAA Rules Applicability

For Covered Entity: - **Privacy Rule:** Applies to all PHI - **Security Rule:** Applies to all ePHI - **Breach Notification Rule:** Applies to all unsecured PHI

For Hybrid Entity: - **Privacy Rule:** Applies only to healthcare components - **Security Rule:** Applies only to healthcare components - **Breach Notification Rule:** Applies only to healthcare components - **Note:** Shared workforce and infrastructure must comply when accessing healthcare component PHI

3.8.2 8.2 Documentation Requirements

Required Documentation: - [ ] Covered entity determination - [ ] Hybrid entity designation (if applicable) - [ ] Healthcare component definitions - [ ] Workforce assignments - [ ] Business associate agreements - [ ] Policies and procedures - [ ] Training records

Documentation Retention: [TODO: 6 years from creation or last effective date]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 4

Business Associates and Subcontractors

Document ID: HIPAA-0030
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

4.1 1. Purpose

This document identifies and manages all Business Associate relationships for AdminSend GmbH and ensures compliance with HIPAA Business Associate requirements.

4.1.1 1.1 Objectives

- **BA Identification:** Identify all entities that meet Business Associate definition
- **BAA Management:** Ensure valid Business Associate Agreements are in place
- **Compliance Monitoring:** Monitor BA compliance with HIPAA requirements
- **Subcontractor Oversight:** Track and manage subcontractor relationships

4.1.2 1.2 References

- **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 liability provisions

4.2 2. Business Associate Definition

4.2.1 2.1 What is a Business Associate?

A Business Associate is a person or entity that: 1. Performs functions or activities on behalf of, or provides services to, a covered entity 2. Involves the use or disclosure of PHI 3. Is not part of the covered entity's workforce

4.2.2 2.2 Common Business Associate Functions

Business Associate Services Include: - Claims processing or administration - Data analysis, processing, or administration - Utilization review - Quality assurance - Billing, benefit management, practice management - Repricing or other services - Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services

Examples of Business Associates: - Third-party administrators - Billing companies - IT service providers (with PHI access) - Cloud storage providers - Shredding companies - Legal counsel (with PHI access) - Consultants (with PHI access) - Data analysis firms

4.2.3 2.3 Entities That Are NOT Business Associates

Conduit Exception: - Telecommunications companies - Internet Service Providers (ISPs) - Postal services - Couriers (if only transporting sealed PHI)

Other Exceptions: - Workforce members - Healthcare providers in treatment relationship - Health plan members - Group health plan sponsors (with certain limitations)

4.3 3. Business Associate Inventory

4.3.1 3.1 Current Business Associates

BA ID	Business Associate Name	Service Provided	PHI Access Type	BAA Status	BAA Date	Review Date
[TODO: BA-001]	[TODO: IT Support Vendor]	IT support and maintenance	ePHI access	[TODO: Active]	[TODO: 2024-01-15]	[TODO: 2027-01-15]
[TODO: BA-002]	[TODO: Billing Service]	Medical billing	PHI processing	[TODO: Active]	[TODO: 2023-06-01]	[TODO: 2026-06-01]
[TODO: BA-003]	[TODO: Cloud Provider]	Data hosting	ePHI storage	[TODO: Active]	[TODO: 2025-03-10]	[TODO: 2028-03-10]
[TODO: BA-004]	[TODO: Transcription Service]	Medical transcription	PHI creation	[TODO: Active]	[TODO: 2024-09-20]	[TODO: 2027-09-20]
[TODO: BA-005]	[TODO: Shredding Company]	Document destruction	Paper PHI	[TODO: Active]	[TODO: 2025-01-05]	[TODO: 2028-01-05]

BA ID	Business Associate Name	Service Provided	PHI Access Type	BAA Status	BAA Date	Review Date
[TODO: BA-006]	[TODO: Legal Firm]	Legal services	PHI review	[TODO: Active]	[TODO: 2024-11-12]	[TODO: 2027-11-12]
[TODO: BA-007]	[TODO: Accounting Firm]	Financial audit	PHI access	[TODO: Active]	[TODO: 2025-02-28]	[TODO: 2028-02-28]

4.3.2 3.2 Business Associate Details

BA-001: [TODO: IT Support Vendor] - **Contact Person:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone] - **Address:** [TODO: Address] - **Services:** [TODO: Detailed description] - **PHI Access:** [TODO: Systems accessed, type of access] - **Subcontractors:** [TODO: Yes/No, list if yes] - **Insurance:** [TODO: Cyber liability coverage amount] - **Compliance Attestation:** [TODO: Date of last attestation]

BA-002: [TODO: Billing Service] - **Contact Person:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone] - **Address:** [TODO: Address] - **Services:** [TODO: Detailed description] - **PHI Access:** [TODO: Data elements accessed] - **Subcontractors:** [TODO: Yes/No, list if yes] - **Insurance:** [TODO: Coverage amount] - **Compliance Attestation:** [TODO: Date]

[TODO: Continue for all Business Associates]

4.4 4. Business Associate Agreements (BAAs)

4.4.1 4.1 BAA Requirements

Required BAA Provisions (45 CFR §164.504(e)):

1. **Permitted Uses and Disclosures:**
   - Specify permitted uses and disclosures of PHI
   - Limit uses/disclosures to those required by contract or law
2. **Safeguards:**
   - Implement appropriate safeguards to prevent unauthorized use/disclosure
   - Comply with Security Rule for ePHI
3. **Subcontractor Requirements:**
   - Ensure subcontractors agree to same restrictions
   - Obtain satisfactory assurances from subcontractors
4. **Reporting:**
   - Report unauthorized uses/disclosures to covered entity
   - Report security incidents
   - Report breaches of unsecured PHI
5. **Individual Rights:**
   - Make PHI available for access requests
   - Make PHI available for amendment requests
   - Provide accounting of disclosures
6. **Compliance:**
   - Make internal practices, books, and records available for HHS compliance review

- Return or destroy PHI at termination (if feasible)

7. **Termination:**
   - Authorize termination if BA violates material term
   - Specify PHI disposition at termination

4.4.2 4.2 BAA Template

Standard BAA Template Location: [TODO: File path or document management system location]

BAA Template Version: [TODO: Version number and date]

Template Approval: - **Approved by Legal:** [TODO: Yes/No, Date] - **Approved by Privacy Officer:** [TODO: Yes/No, Date] - **Approved by Compliance:** [TODO: Yes/No, Date]

4.4.3 4.3 BAA Execution Process

Process Steps: 1. Identify need for Business Associate relationship 2. Conduct BA due diligence and risk assessment 3. Negotiate services agreement 4. Execute Business Associate Agreement 5. Document BAA in inventory 6. Monitor BA compliance 7. Review BAA periodically (at least every 3 years)

Approval Authority: - **Services < $10,000:** [TODO: Department Manager] - **Services $10,000-$50,000:** [TODO: Director + Privacy Officer] - **Services > $50,000:** [TODO: Executive + Privacy Officer + Legal]

4.5 5. Subcontractor Management

4.5.1 5.1 Subcontractor Requirements

HIPAA Requirements for Subcontractors: - Business Associates must obtain satisfactory assurances from subcontractors - Subcontractors must enter into BAA with Business Associate - Subcontractors have same HIPAA obligations as Business Associates - Covered Entity must be notified of subcontractor arrangements

4.5.2 5.2 Subcontractor Inventory

Subcontractor	Primary BA	Service	PHI Access	BAA with BA	CE Notified
[TODO: Cloud Backup Provider]	[TODO: IT Vendor]	Data backup	ePHI	[TODO: Yes]	[TODO: Yes, Date]
[TODO: Offshore Support]	[TODO: IT Vendor]	Help desk	ePHI	[TODO: Yes]	[TODO: Yes, Date]
[TODO: Courier Service]	[TODO: Lab]	Specimen transport	Paper PHI	[TODO: Yes]	[TODO: Yes, Date]

4.5.3 5.3 Subcontractor Approval Process

Covered Entity Approval Required: [TODO: Yes/No]

Approval Process: 1. Business Associate requests approval to use subcontractor 2. BA provides subcontractor information and proposed BAA 3. Privacy Officer reviews subcontractor arrangement 4. Approval granted or denied within [TODO: 10 business days] 5. BA executes BAA with subcontractor 6. BA provides copy of executed BAA to Covered Entity

4.6 6. Business Associate Due Diligence

4.6.1 6.1 Pre-Engagement Assessment

Due Diligence Checklist: - [ ] Business Associate questionnaire completed - [ ] HIPAA compliance attestation received - [ ] Security controls documentation reviewed - [ ] Incident response plan reviewed - [ ] Breach notification procedures reviewed - [ ] Insurance coverage verified (cyber liability) - [ ] References checked - [ ] Financial stability assessed - [ ] Subcontractor list provided

Risk Assessment: | Risk Factor | Assessment | Mitigation | |————-|————|————| | [TODO: Data volume] | [TODO: High/Medium/Low] | [TODO: Mitigation measures] | | [TODO: Sensitivity of PHI] | [TODO: High/Medium/Low] | [TODO: Mitigation measures] | | [TODO: Security maturity] | [TODO: High/Medium/Low] | [TODO: Mitigation measures] |

4.6.2 6.2 Ongoing Monitoring

Monitoring Activities: - Annual compliance attestation - Periodic security assessments - Breach notification tracking - Incident review - Performance reviews - Contract compliance audits

Monitoring Schedule: | Activity | Frequency | Responsible Party | Last Completed | |———-|———–|——————-|——————-| | [TODO: Compliance attestation] | Annual | [TODO: Privacy Officer] | [TODO: Date] | | [TODO: Security assessment] | Annual | [TODO: Security Officer] | [TODO: Date] | | [TODO: Performance review] | Quarterly | [TODO: Contract Manager] | [TODO: Date] |

4.7 7. Breach Notification from Business Associates

4.7.1 7.1 BA Breach Notification Requirements

Business Associates Must Notify Covered Entity: - **Timing:** Without unreasonable delay, no later than 60 days from discovery - **Method:** Written notification (email acceptable) - **Content:** - Identification of each individual affected - Description of breach - Types of PHI involved - Date of breach and discovery date - Steps individuals should take - BA's investigation and mitigation efforts

4.7.2 7.2 Breach Notification Log

Breach ID	BA Name	Discovery Date	Notification Date	Individuals Affected	PHI Involved	Status
[TODO: BR-001]	[TODO: BA Name]	[TODO: Date]	[TODO: Date]	[TODO: Number]	[TODO: Types]	[TODO: Resolved]

4.7.3 7.3 Breach Response Process

Upon Receiving BA Breach Notification: 1. Acknowledge receipt of notification 2. Request additional information if needed 3. Assess breach for reporting requirements 4. Notify affected individuals (if required) 5. Notify HHS (if required) 6. Notify media (if required - 500+ individuals) 7. Document breach and response 8. Review BA relationship and controls

4.8 8. Business Associate Termination

4.8.1 8.1 Termination Triggers

Grounds for Termination: - Material breach of BAA - Failure to cure breach within specified timeframe - Repeated security incidents - Failure to report breaches - Insolvency or bankruptcy - End of service relationship

4.8.2 8.2 Termination Process

Termination Steps: 1. Provide written notice of termination 2. Specify termination date 3. Request return or destruction of PHI 4. Verify PHI return/destruction 5. Obtain certification of destruction (if applicable) 6. Update Business Associate inventory 7. Notify affected systems/departments 8. Conduct post-termination review

4.8.3 8.3 PHI Disposition

Options at Termination: - **Return PHI:** BA returns all PHI to Covered Entity - **Destroy PHI:** BA destroys PHI and provides certification - **Retain PHI:** If return/destruction not feasible, BA retains PHI with continued protections

Retention Justification: [TODO: Document reasons if PHI retention is necessary]

4.9 9. Compliance and Audit

4.9.1 9.1 BA Compliance Monitoring

Monitoring Methods: - Annual compliance attestations - On-site audits (if contractually permitted) - Security assessments - Penetration testing results review - SOC 2 reports review - ISO 27001 certifications review

Audit Rights: - Covered Entity reserves right to audit BA compliance - Audit frequency: [TODO: Annual or as needed] - Audit scope: HIPAA compliance, security controls, BAA compliance

4.9.2 9.2 Documentation and Records

Required Documentation: - Executed Business Associate Agreements - Due diligence assessments - Compliance attestations - Breach notifications - Audit reports - Correspondence regarding PHI

Retention Period: [TODO: 6 years from creation or last effective date]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 5

Roles and Responsibilities

Document ID: HIPAA-0040
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

5.1 1. Purpose

This document defines the roles, responsibilities, and accountabilities for HIPAA compliance at AdminSend GmbH.

5.1.1 1.1 Objectives

- **Role Definition:** Clearly define HIPAA-required and supporting roles
- **Accountability:** Establish decision-making authority
- **Compliance:** Meet HIPAA requirements for designated officials
- **Communication:** Establish clear communication and escalation paths

5.1.2 1.2 HIPAA-Required Roles

HIPAA Mandates: - **Privacy Officer** (45 CFR §164.530(a)(1)(i)) - Required - **Security Officer** (45 CFR §164.308(a)(2)) - Required - **Contact Person** for individual rights (45 CFR §164.530(a)(1)(ii)) - Required

5.2 2. Executive Leadership

5.2.1 2.1 Chief Executive Officer (CEO)

Name: {{ meta.roles.ceo.name }}
Email: {{ meta.roles.ceo.email }}
Phone: {{ meta.roles.ceo.phone }}

Responsibilities: - Ultimate accountability for HIPAA compliance - Approval of HIPAA policies and procedures - Allocation of resources for compliance program - Oversight of Privacy and Security Officers - Final escalation point for compliance issues - Approval of sanctions for policy violations

5.2.2 2.2 Chief Information Officer (CIO)

Name: {{ meta.roles.cio.name }}
Email: {{ meta.roles.cio.email }}
Phone: {{ meta.roles.cio.phone }}

Responsibilities: - IT infrastructure supporting HIPAA compliance - Technology investments for security and privacy - Oversight of Security Officer - Approval of technical safeguards - IT risk management

5.2.3 2.3 Chief Compliance Officer (CCO)

Name: [TODO: Name]
Email: [TODO: Email]
Phone: [TODO: Phone]

Responsibilities: - Overall compliance program oversight - Coordination of Privacy and Security functions - Regulatory monitoring and updates - Compliance reporting to Board/Executive team - Internal audit program oversight

5.3 3. HIPAA-Required Roles

5.3.1 3.1 Privacy Officer

Name: {{ meta.roles.privacy_officer.name }}
Email: {{ meta.roles.privacy_officer.email }}
Phone: {{ meta.roles.privacy_officer.phone }}
Office Location: [TODO: Location]

HIPAA Requirement: 45 CFR §164.530(a)(1)(i)

Responsibilities: - Development and implementation of privacy policies and procedures - Privacy training program management - Investigation of privacy complaints - Privacy incident response - Individual rights request processing (access, amendment, accounting) - Business Associate Agreement oversight - Privacy risk assessments - Notice of Privacy Practices maintenance - Privacy compliance monitoring - Liaison with HHS Office for Civil Rights (OCR)

Authority: - Access to all PHI and systems - Authority to investigate privacy matters - Recommend sanctions for privacy violations - Approve privacy-related policies - Halt activities that violate privacy requirements

Backup Privacy Officer: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

5.3.2 3.2 Security Officer

Name: {{ meta.roles.security_officer.name }}
Email: {{ meta.roles.security_officer.email }}
Phone: {{ meta.roles.security_officer.phone }}
Office Location: [TODO: Location]

HIPAA Requirement: 45 CFR §164.308(a)(2)

Responsibilities: - Development and implementation of security policies and procedures - Security risk analysis and risk management - Security training program management - Security incident response - Technical, physical, and administrative safeguards implementation - Access control management - Audit log review and monitoring - Vulnerability management - Security compliance monitoring - Liaison with security vendors and consultants

Authority: - Access to all systems and security controls - Authority to investigate security incidents - Recommend sanctions for security violations - Approve security-related policies - Emergency authority to disable access or systems

Backup Security Officer: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

5.3.3 3.3 Contact Person for Individual Rights

Name: [TODO: Name]
Email: [TODO: Email]
Phone: [TODO: Phone]
Mailing Address: [TODO: Address]

HIPAA Requirement: 45 CFR §164.530(a)(1)(ii)

Responsibilities: - Receive and process requests for access to PHI - Receive and process requests for amendment of PHI - Receive and process requests for accounting of disclosures - Receive and process requests for restrictions - Receive and process requests for confidential communications - Receive privacy complaints - Provide Notice of Privacy Practices

Note: This role may be filled by the Privacy Officer or designee.

5.4 4. Supporting Roles

5.4.1 4.1 HIPAA Compliance Manager

Name: [TODO: Name]
Email: [TODO: Email]
Phone: [TODO: Phone]

Responsibilities: - Day-to-day HIPAA compliance program management - Policy and procedure maintenance - Training coordination - Compliance monitoring and auditing - Documentation management - Vendor management support - Compliance reporting

5.4.2 4.2 IT Security Manager

Name: [TODO: Name]
Email: [TODO: Email]
Phone: [TODO: Phone]

Responsibilities: - Implementation of technical safeguards - Access control administration - Security monitoring and logging - Vulnerability scanning and remediation - Patch management - Encryption implementation - Network security - Incident response (technical)

5.4.3 4.3 System Administrators

Team Size: [TODO: Number]
Team Lead: [TODO: Name]
Contact: [TODO: Email]

Responsibilities: - System configuration and maintenance - User account management - Backup and recovery - System hardening - Security update implementation - Audit log management - System monitoring

5.4.4 4.4 Privacy Coordinators (by Department)

Department	Coordinator	Email	Phone
[TODO: Clinical]	[TODO: Name]	[TODO: Email]	[TODO: Phone]
[TODO: Billing]	[TODO: Name]	[TODO: Email]	[TODO: Phone]
[TODO: IT]	[TODO: Name]	[TODO: Email]	[TODO: Phone]
[TODO: HR]	[TODO: Name]	[TODO: Email]	[TODO: Phone]

Responsibilities: - Department-level privacy compliance - Privacy training coordination - Privacy incident reporting - Policy implementation support - Liaison with Privacy Officer

5.4.5 4.5 Human Resources

HR Director: [TODO: Name]
Email: [TODO: Email]
Phone: [TODO: Phone]

Responsibilities: - Background checks for workforce with PHI access - Onboarding and offboarding processes - Confidentiality agreements - Training record maintenance - Sanctions and disciplinary actions - Workforce security

5.4.6 4.6 Legal Counsel

Name: [TODO: Name]
Firm: [TODO: Firm name]
Email: [TODO: Email]
Phone: [TODO: Phone]

Responsibilities: - Legal advice on HIPAA matters - Contract review (BAAs, vendor agreements) - Breach notification legal review - OCR investigation support - Regulatory interpretation - Litigation support

5.4.7 4.7 Risk Management

Risk Manager: [TODO: Name]
Email: [TODO: Email]
Phone: [TODO: Phone]

Responsibilities: - HIPAA risk assessments - Risk mitigation planning - Insurance coverage (cyber liability) - Incident investigation support - Risk reporting

5.5 5. RACI Matrices

5.5.1 5.1 Privacy Rule Compliance

Activity	CEO	Privacy Officer	Security Officer	Dept Managers	Legal
Privacy policies	A	R	C	C	C
Notice of Privacy Practices	A	R	I	I	C
Individual access requests	I	A/R	I	C	C
Privacy complaints	I	A/R	I	C	C
Privacy training	A	R	C	C	I
Privacy incidents	I	A/R	C	C	C
BAA management	A	R	C	C	R

5.5.2 5.2 Security Rule Compliance

Activity	CEO	Privacy Officer	Security Officer	IT Manager	Dept Managers
Security policies	A	C	R	C	C
Risk analysis	A	C	R	C	C
Access control	I	C	A/R	R	C
Audit controls	I	C	A/R	R	I

Activity	CEO	Privacy Officer	Security Officer	IT Manager	Dept Managers
Security incidents	I	C	A/R	R	C
Security training	A	C	R	C	C
Vulnerability management	I	I	A	R	I

5.5.3 5.3 Breach Notification

Activity	CEO	Privacy Officer	Security Officer	Legal	PR/Communications
Breach assessment	I	A/R	R	C	I
Individual notification	A	R	C	C	C
HHS notification	A	R	C	C	I
Media notification	A	R	I	C	R
Breach investigation	I	A	R	C	I
Remediation	A	C	R	C	I

Legend: - **R** (Responsible): Performs the work - **A** (Accountable): Ultimate accountability, approves work (only one A per activity) - **C** (Consulted): Provides input, two-way communication - **I** (Informed): Kept informed, one-way communication

5.6 6. HIPAA Compliance Committee

5.6.1 6.1 Committee Structure

Committee Name: HIPAA Compliance Committee

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

Members: - CEO or designee - Privacy Officer - Security Officer - CIO or IT Director - Compliance Officer - Legal Counsel - Risk Manager - HR Director - Clinical Director (if applicable) - Department representatives

Meeting Frequency: [TODO: Monthly/Quarterly]

Quorum: [TODO: Minimum number of members]

5.6.2 6.2 Committee Responsibilities

- Oversight of HIPAA compliance program
- Review and approval of policies and procedures

- Review of risk assessments and mitigation plans
- Review of privacy and security incidents
- Review of training effectiveness
- Budget recommendations for compliance activities
- Regulatory update review
- Audit findings review
- Continuous improvement initiatives

5.6.3 6.3 Meeting Documentation

Meeting Minutes: - Attendance - Topics discussed - Decisions made - Action items assigned - Follow-up required

Minutes Retention: [TODO: 6 years]

5.7 7. Escalation Procedures

5.7.1 7.1 Privacy Incident Escalation

Level 1: Privacy Coordinator (Department)
Level 2: Privacy Officer
Level 3: CEO + Legal Counsel

Escalation Criteria: - Suspected breach of unsecured PHI - Unauthorized access to PHI - Privacy complaint from individual - OCR investigation - Media inquiry

Response Time: - Level 1: Immediate - Level 2: Within 1 hour - Level 3: Within 4 hours

5.7.2 7.2 Security Incident Escalation

Level 1: IT Help Desk / System Administrator
Level 2: Security Officer
Level 3: CIO + CEO

Escalation Criteria: - Suspected security breach - Malware infection - Unauthorized system access - System compromise - Data exfiltration - Ransomware

Response Time: - Level 1: Immediate - Level 2: Within 30 minutes - Level 3: Within 1 hour

5.7.3 7.3 24/7 Contact Information

Security Hotline: [TODO: Phone number]
Privacy Hotline: [TODO: Phone number]
After-Hours Contact: [TODO: On-call rotation or answering service]

Emergency Contacts: | Role | Name | Mobile | Email | |——|——|——–|——-| | Privacy Officer | {{ meta.roles.privacy_officer.name }} | [TODO: Mobile] | {{ meta.roles.privacy_officer.email }} | | Security Officer | {{ meta.roles.security_officer.name }} | [TODO: Mobile] | {{ meta.roles.security_officer.email }} | | CEO | {{ meta.roles.ceo.name }} | [TODO: Mobile] | {{ meta.roles.ceo.email }} |

5.8 8. Training and Competency

5.8.1 8.1 Role-Specific Training

Role	Training Required	Frequency	Provider
All Workforce	HIPAA Basics	Annual	[TODO: LMS/Vendor]
Privacy Officer	Privacy Rule Deep Dive	Annual	[TODO: External]
Security Officer	Security Rule Deep Dive	Annual	[TODO: External]
IT Staff	Technical Safeguards	Annual	[TODO: Internal/External]
Clinical Staff	PHI Handling	Annual	[TODO: Internal]
Managers	Workforce Management	Annual	[TODO: Internal]

5.8.2 8.2 Competency Requirements

Privacy Officer: - Knowledge of HIPAA Privacy Rule - Understanding of healthcare operations - Investigation skills - Communication skills - Policy development experience

Security Officer: - Knowledge of HIPAA Security Rule - Technical security expertise - Risk assessment skills - Incident response experience - Security architecture knowledge

5.9 9. Performance Metrics

5.9.1 9.1 Compliance Metrics

Metric	Target	Measurement	Responsible
Training completion rate	100%	Quarterly	Privacy Officer
Incident response time	$<$ 1 hour	Per incident	Security Officer
Access request response time	$<$ 30 days	Per request	Privacy Officer
Risk assessment completion	Annual	Annual	Security Officer
Policy review completion	Annual	Annual	Compliance Manager

5.9.2 9.2 Reporting

Monthly Reports: - Privacy incidents - Security incidents - Training completion - Access requests processed

Quarterly Reports: - Compliance metrics - Risk assessment updates - Audit findings - Improvement initiatives

Annual Reports: - Comprehensive compliance review - Risk analysis results - Training effectiveness - Budget and resource needs

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 6

HIPAA Compliance Program

Document ID: HIPAA-0050
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

6.1 1. Purpose

This document describes the HIPAA compliance program for AdminSend GmbH, including program structure, activities, monitoring, and continuous improvement processes.

6.1.1 1.1 Objectives

- **Program Framework:** Establish comprehensive HIPAA compliance program
- **Systematic Approach:** Define structured compliance activities
- **Continuous Improvement:** Implement ongoing monitoring and enhancement
- **Accountability:** Assign clear responsibilities for compliance activities

6.1.2 1.2 Program Scope

HIPAA Rules Covered: - 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 Program Structure

6.2.1 2.1 Program Components

1. Governance and Leadership - Executive oversight - Privacy and Security Officers - HIPAA Compliance Committee - Resource allocation

2. Policies and Procedures - Privacy policies - Security policies - Breach notification procedures - Workforce policies

3. Risk Management - Risk analysis - Risk management - Risk mitigation - Ongoing risk assessment

4. Training and Awareness - Initial training - Annual training - Role-specific training - Awareness campaigns

5. Monitoring and Auditing - Compliance monitoring - Internal audits - External assessments - Corrective actions

6. Incident Management - Privacy incidents - Security incidents - Breach assessment - Breach notification

7. Business Associate Management - BA identification - BAA execution - BA monitoring - BA termination

8. Individual Rights - Access requests - Amendment requests - Accounting of disclosures - Restriction requests - Confidential communications

9. Documentation and Records - Policy documentation - Training records - Incident records - Audit records

10. Continuous Improvement - Program assessment - Lessons learned - Best practices - Regulatory updates

6.2.2 2.2 Program Organization

```
CEO
    Privacy Officer
        Privacy Coordinators
        Individual Rights Processing
        Privacy Incident Response
    Security Officer
        IT Security Team
        Access Control Management
        Security Incident Response
    Compliance Officer
         Compliance Manager
         Training Coordinator
         Audit Coordinator
```

6.3 3. Compliance Program Activities

6.3.1 3.1 Annual Activities

Activity	Responsible	Timeline	Deliverable
Risk Analysis	Security Officer	Q1	Risk Analysis Report
Policy Review	Privacy Officer	Q2	Updated Policies
Internal Audit	Compliance Manager	Q3	Audit Report
Training Program Review	Privacy Officer	Q4	Training Assessment
Program Assessment	Compliance Officer	Q4	Annual Report
Management Review	CEO	Q4	Management Review Minutes

6.3.2 3.2 Quarterly Activities

Activity	Responsible	Deliverable
Compliance Committee Meeting	Privacy Officer	Meeting Minutes
Metrics Review	Compliance Manager	Metrics Dashboard
BA Compliance Review	Privacy Officer	BA Status Report
Incident Trend Analysis	Security Officer	Incident Report
Training Completion Review	Training Coordinator	Training Report

6.3.3 3.3 Monthly Activities

Activity	Responsible	Deliverable
Access Review	Security Officer	Access Review Report
Audit Log Review	IT Security	Log Review Summary
Incident Review	Privacy/Security Officers	Incident Summary
Training Tracking	Training Coordinator	Training Status
Policy Updates	Compliance Manager	Change Log

6.3.4 3.4 Ongoing Activities

Activity	Responsible	Frequency
Individual Rights Requests	Privacy Officer	As received
Privacy Complaints	Privacy Officer	As received
Security Incidents	Security Officer	As detected
Privacy Incidents	Privacy Officer	As detected
Breach Assessment	Privacy/Security Officers	As needed
Workforce Onboarding	HR + Privacy Officer	As needed
Workforce Offboarding	HR + Security Officer	As needed

6.4 4. Policies and Procedures

6.4.1 4.1 Policy Framework

Policy Hierarchy: 1. **HIPAA Compliance Policy** (This document) 2. **Privacy Policies** (HIPAA-0500 series) 3. **Security Policies** (HIPAA-0100-0400 series) 4. **Operational Procedures** (Department-specific) 5. **Work Instructions** (Task-specific)

6.4.2 4.2 Policy Development Process

Process Steps: 1. Identify need for policy 2. Draft policy (Privacy/Security Officer) 3. Stakeholder review 4. Legal review 5. Compliance Committee approval 6. Executive approval 7. Communication and training 8. Implementation 9. Monitoring and enforcement

Policy Template: [TODO: Reference to policy template]

6.4.3 4.3 Policy Review and Update

Review Schedule: - **Annual Review:** All policies reviewed annually - **Triggered Review:** When regulations change, incidents occur, or operations change - **Version Control:** All policies version-controlled

Review Process: 1. Privacy/Security Officer initiates review 2. Assess current policy effectiveness 3. Identify needed changes 4. Update policy 5. Repeat approval process 6. Communicate changes 7. Update training materials

6.4.4 4.4 Policy Inventory

Policy ID	Policy Name	Owner	Last Review	Next Review
HIPAA-0050	HIPAA Compliance Program	Privacy Officer	[TODO: Date]	[TODO: Date]
HIPAA-0100	Security Management Process	Security Officer	[TODO: Date]	[TODO: Date]
HIPAA-0500	Privacy Practices	Privacy Officer	[TODO: Date]	[TODO: Date]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

6.5 5. Training Program

6.5.1 5.1 Training Requirements

HIPAA Training Required For: - All workforce members (employees, volunteers, trainees, contractors) - Business associates (recommended) - New hires (within 30 days) - Annual refresher training - When policies change significantly

Training Topics: - HIPAA overview and applicability - Privacy Rule requirements - Security Rule requirements - Breach Notification Rule - Individual rights - Permitted uses and disclosures - Minimum necessary standard - Authorization requirements - Security safeguards - Incident reporting - Sanctions for violations - Organization-specific policies

6.5.2 5.2 Training Delivery

Training Methods: - Online learning management system (LMS) - In-person sessions - Department meetings - New hire orientation - Role-specific training - Just-in-time training

Training Materials: - Training modules - Quick reference guides - Posters and reminders - Email communications - Intranet resources

6.5.3 5.3 Training Tracking

Documentation Required: - Training attendance records - Training completion certificates - Test scores (if applicable) - Training materials provided - Training dates and duration

Retention: [TODO: 6 years]

Training Database: [TODO: LMS or tracking system]

6.6 6. Monitoring and Auditing

6.6.1 6.1 Compliance Monitoring

Monitoring Activities: - Access log reviews - Audit trail reviews - Policy compliance checks - Security control testing - Privacy practice observations - Complaint investigations - Incident reviews

Monitoring Schedule: | Activity | Frequency | Responsible | |———-|———-|———-| | Access log review | Monthly | Security Officer | | Audit trail review | Monthly | IT Security | | Policy compliance spot checks | Quarterly | Compliance Manager | | Security control testing | Quarterly | Security Officer | | Privacy practice audits | Semi-annual | Privacy Officer |

6.6.2 6.2 Internal Audit Program

Audit Scope: - Privacy Rule compliance - Security Rule compliance - Breach Notification compliance - Policy adherence - Training effectiveness - Business Associate management - Individual rights processing - Documentation and records

Audit Frequency: Annual (minimum)

Audit Process: 1. Develop audit plan 2. Notify auditees 3. Conduct audit (interviews, document review, testing) 4. Document findings 5. Report results 6. Develop corrective action plan 7. Implement corrections 8. Verify corrections 9. Close audit

Audit Documentation: - Audit plan - Audit checklist - Findings and observations - Corrective action plan - Follow-up verification

6.6.3 6.3 External Assessments

Types of External Assessments: - OCR compliance reviews - OCR audits - Third-party security assessments - Penetration testing - Vulnerability assessments - Certification audits (e.g., HITRUST)

Preparation for External Assessments: - Maintain current documentation - Conduct pre-assessment readiness review - Assign assessment coordinator - Prepare evidence repository - Brief workforce - Coordinate logistics

6.7 7. Incident Management

6.7.1 7.1 Incident Types

Privacy Incidents: - Unauthorized access to PHI - Unauthorized disclosure of PHI - Improper use of PHI - Loss or theft of PHI - Privacy complaints

Security Incidents: - Unauthorized system access - Malware infection - Phishing attacks - Lost or stolen devices - System vulnerabilities - Denial of service

6.7.2 7.2 Incident Response Process

Process Steps: 1. **Detection and Reporting** - Incident identified - Reported to Privacy/Security Officer - Initial assessment

2. **Containment**
   - Stop ongoing incident
   - Prevent further damage
   - Preserve evidence
3. **Investigation**
   - Determine scope and impact
   - Identify root cause
   - Document findings
4. **Breach Assessment**
   - Apply breach risk assessment
   - Determine if breach occurred
   - Assess notification requirements
5. **Notification** (if breach)
   - Notify individuals
   - Notify HHS
   - Notify media (if 500+ individuals)
6. **Remediation**
   - Implement corrective actions
   - Mitigate vulnerabilities
   - Update controls
7. **Documentation**
   - Incident report
   - Investigation findings
   - Actions taken
   - Lessons learned
8. **Follow-up**
   - Monitor for recurrence
   - Verify effectiveness of corrections
   - Update policies/procedures

6.7.3 7.3 Incident Documentation

Required Documentation: - Incident report form - Investigation notes - Breach risk assessment - Notification records - Remediation plan - Lessons learned

Retention: [TODO: 6 years]

6.8 8. Metrics and Reporting

6.8.1 8.1 Key Performance Indicators (KPIs)

KPI	Target	Measurement	Frequency
Training completion rate	100%	% workforce trained	Quarterly
Incident response time	< 1 hour	Time to containment	Per incident
Access request response time	< 30 days	Days to fulfill	Per request
Risk assessment completion	100%	Annual completion	Annual
Policy review completion	100%	% policies reviewed	Annual
Audit findings closure	< 90 days	Days to close	Per finding
BA BAA coverage	100%	% BAs with current BAA	Quarterly

6.8.2 8.2 Reporting Structure

Monthly Reports: - Incident summary - Training status - Access requests processed - Metrics dashboard

Quarterly Reports: - Compliance metrics - Audit status - Risk updates - BA compliance

Annual Reports: - Comprehensive program review - Risk analysis results - Training effectiveness - Audit findings - Improvement initiatives - Budget and resources

Report Recipients: - CEO - Compliance Committee - Board of Directors (annual) - Department managers (relevant sections)

6.9 9. Continuous Improvement

6.9.1 9.1 Improvement Process

Improvement Sources: - Incident lessons learned - Audit findings - Regulatory changes - Industry best practices - Technology advances - Workforce feedback

Improvement Cycle: 1. Identify improvement opportunity 2. Assess current state 3. Define desired state 4. Develop improvement plan 5. Implement changes 6. Monitor effectiveness 7. Standardize improvements 8. Document and communicate

6.9.2 9.2 Regulatory Monitoring

Monitoring Activities: - HHS website monitoring - Federal Register monitoring - Industry association updates - Legal counsel updates - Compliance newsletters - Webinars and conferences

Regulatory Change Process: 1. Identify regulatory change 2. Assess impact on organization 3. Develop compliance plan 4. Update policies and procedures 5. Train workforce 6. Implement changes 7. Monitor compliance

6.10 10. Program Assessment

6.10.1 10.1 Annual Program Assessment

Assessment Components: - Program effectiveness review - Goal achievement assessment - Resource adequacy review - Stakeholder feedback - Benchmarking against industry - Gap analysis

Assessment Process: 1. Collect data (metrics, audit results, incidents) 2. Analyze trends 3. Identify strengths and weaknesses 4. Develop recommendations 5. Present to Compliance Committee 6. Present to Executive Leadership 7. Develop improvement plan 8. Allocate resources 9. Implement improvements

6.10.2 10.2 Management Review

Management Review Meeting: - **Frequency:** Annual (minimum) - **Participants:** CEO, Privacy Officer, Security Officer, Compliance Officer, Department Heads - **Agenda:** - Program performance review - Incident and breach review - Audit findings review - Resource needs - Regulatory changes - Improvement initiatives - Goals for next year

Management Review Documentation: - Meeting minutes - Decisions made - Action items assigned - Resource commitments

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 7

Security Management Process

Document ID: HIPAA-0100
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

7.1 1. Purpose

This document describes the Security Management Process for AdminSend GmbH, including risk analysis, risk management, sanction policy, and information system activity review as required by HIPAA Security Rule §164.308(a)(1).

7.1.1 1.1 HIPAA Requirement

Standard: §164.308(a)(1) - Security Management Process (Required)

Implementation Specifications: - §164.308(a)(1)(ii)(A) - Risk Analysis (Required) - §164.308(a)(1)(ii)(B) - Risk Management (Required) - §164.308(a)(1)(ii)(C) - Sanction Policy (Required) - §164.308(a)(1)(ii)(D) - Information System Activity Review (Required)

7.2 2. Risk Analysis

7.2.1 2.1 Risk Analysis Process

Requirement: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

Process Steps: 1. **Scope Definition** - Identify all ePHI within organization - Define systems, applications, and locations - Identify workforce with ePHI access

2. **Data Collection**
   - Inventory IT assets
   - Document data flows
   - Identify current security measures
   - Review policies and procedures
3. **Threat Identification**
   - Natural threats (fire, flood, earthquake)
   - Human threats (unauthorized access, malicious insider, social engineering)
   - Environmental threats (power failure, hardware failure)
4. **Vulnerability Assessment**
   - Technical vulnerabilities
   - Physical vulnerabilities
   - Administrative vulnerabilities
5. **Risk Determination**
   - Likelihood assessment
   - Impact assessment
   - Risk level calculation
6. **Documentation**
   - Risk analysis report
   - Risk register
   - Recommendations

Frequency: Annual (minimum) or when significant changes occur

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

7.2.2 2.2 Risk Analysis Methodology

Risk Assessment Formula:

```
Risk = Likelihood × Impact
```

Likelihood Scale: - **High (3):** Very likely to occur (> 50% probability) - **Medium (2):** Possible to occur (10-50% probability) - **Low (1):** Unlikely to occur (< 10% probability)

Impact Scale: - **High (3):** Severe impact on confidentiality, integrity, or availability - **Medium (2):** Moderate impact - **Low (1):** Minimal impact

Risk Levels: - **Critical (7-9):** Immediate action required - **High (5-6):** Action required within 30 days - **Medium (3-4):** Action required within 90 days - **Low (1-2):** Monitor and review

7.2.3 2.3 Risk Register

Risk ID	Threat	Vulnerability	Likelihood	Impact	Risk Level	Mitigation	Owner	Status
[TODO: R-001]	[TODO: Unauthorized access]	[TODO: Weak passwords]	[TODO: High]	[TODO: High]	[TODO: Critical]	[TODO: Implement MFA]	[TODO: Security Officer]	[TODO: Open]

Risk ID	Threat	Vulnerability	Likelihood	Impact	Risk Level	Mitigation	Owner	Status
[TODO: R-002]	[TODO: Malware]	[TODO: No endpoint protection]	[TODO: Medium]	[TODO: High]	[TODO: High]	[TODO: Deploy EDR]	[TODO: IT Manager]	[TODO: In Progress]

7.3 3. Risk Management

7.3.1 3.1 Risk Management Process

Requirement: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Risk Treatment Options: 1. **Mitigate:** Implement controls to reduce risk 2. **Accept:** Accept risk if within acceptable level 3. **Transfer:** Transfer risk (e.g., insurance, outsourcing) 4. **Avoid:** Eliminate the activity causing the risk

7.3.2 3.2 Risk Mitigation Plan

Risk ID	Mitigation Strategy	Controls to Implement	Timeline	Budget	Responsible	Status
[TODO: R-001]	Mitigate	Multi-factor authentication	[TODO: 30 days]	[TODO: $X]	[TODO: Security Officer]	[TODO: Planned]
[TODO: R-002]	Mitigate	Endpoint detection and response	[TODO: 60 days]	[TODO: $X]	[TODO: IT Manager]	[TODO: In Progress]

7.3.3 3.3 Residual Risk

Residual Risk Assessment: After implementing controls, reassess risk levels to determine residual risk.

Risk ID	Initial Risk Level	Controls Implemented	Residual Risk Level	Acceptance
[TODO: R-001]	Critical (9)	MFA, password policy	Medium (4)	Accepted
[TODO: R-002]	High (6)	EDR, antivirus	Low (2)	Accepted

Risk Acceptance: - Residual risks must be formally accepted by management - Acceptance documented with justification - Periodic review of accepted risks

7.4 4. Sanction Policy

7.4.1 4.1 Policy Statement

Requirement: Apply appropriate sanctions against workforce members who fail to comply with security policies and procedures.

Policy: AdminSend GmbH will apply appropriate sanctions against workforce members who violate HIPAA security policies and procedures. Sanctions will be applied consistently and fairly, commensurate with the severity of the violation.

7.4.2 4.2 Violations and Sanctions

Types of Violations:

Level 1 - Minor Violations: - Unintentional, isolated policy violation - No harm to ePHI - Examples: Leaving workstation unlocked, password written down

Sanctions: - Verbal warning - Mandatory retraining - Documentation in personnel file

Level 2 - Moderate Violations: - Repeated minor violations - Negligent behavior - Examples: Repeated password sharing, accessing unnecessary ePHI

Sanctions: - Written warning - Mandatory retraining - Suspension of system access (temporary) - Performance improvement plan

Level 3 - Serious Violations: - Intentional policy violation - Potential harm to ePHI - Examples: Unauthorized disclosure, accessing ePHI without authorization

Sanctions: - Suspension without pay - Termination of employment - Revocation of system access - Legal action (if applicable)

Level 4 - Critical Violations: - Intentional breach of ePHI - Criminal activity - Examples: Theft of ePHI, selling ePHI, malicious destruction

Sanctions: - Immediate termination - Legal prosecution - Reporting to law enforcement - Reporting to HHS OCR

7.4.3 4.3 Sanction Process

Process Steps: 1. **Incident Discovery:** Violation identified 2. **Investigation:** Security Officer investigates 3. **Determination:** Determine violation level 4. **Consultation:** Consult with HR and Legal 5. **Sanction Decision:** Management decides appropriate sanction 6. **Implementation:** Apply sanction 7. **Documentation:** Document in personnel file and incident log 8. **Follow-up:** Monitor for recurrence

Due Process: - Workforce member notified of alleged violation - Opportunity to respond - Fair and impartial investigation - Consistent application of sanctions

7.4.4 4.4 Sanction Log

Date	Employee ID	Violation	Level	Sanction Applied	Applied By	Status
[TODO: Date]	[TODO: EMP-XXX]	[TODO: Description]	[TODO: Level]	[TODO: Sanction]	[TODO: Manager]	[TODO: Closed]

Retention: [TODO: 6 years]

7.5 5. Information System Activity Review

7.5.1 5.1 Review Requirements

Requirement: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Purpose: - Detect security incidents - Identify policy violations - Monitor system performance - Support investigations - Demonstrate compliance

7.5.2 5.2 Review Activities

Daily Reviews: - Failed login attempts - Critical system alerts - Security tool alerts (IDS/IPS, antivirus) - Privileged account activity

Weekly Reviews: - Access logs for sensitive systems - User account changes - Firewall logs - VPN access logs

Monthly Reviews: - Comprehensive audit log review - Access rights review - Security incident trends - Policy compliance checks

Quarterly Reviews: - User access recertification - Privileged account review - Security control effectiveness - Risk assessment updates

7.5.3 5.3 Audit Log Requirements

Systems Requiring Audit Logging: - All systems containing ePHI - Authentication systems - Network devices (firewalls, routers) - Database systems - Application servers - Email systems

Events to Log: - User login/logout - Access to ePHI - Changes to ePHI - User account changes - Permission changes - System configuration changes - Security events (failed logins, malware detection)

Log Retention: [TODO: 6 years minimum]

7.5.4 5.4 Review Documentation

Review Log: | Review Date | Reviewer | Systems Reviewed | Findings | Actions Taken | Follow-up Required | |————-|———-|——————|———-|——————|——————-| | [TODO: Date] | [TODO: Name] | [TODO: Systems] | [TODO: Findings] | [TODO: Actions] | [TODO: Yes/No] |

Findings and Actions: - Document all findings - Assign corrective actions - Track to completion - Escalate significant findings

7.6 6. Documentation and Records

7.6.1 6.1 Required Documentation

- Risk analysis reports
- Risk register
- Risk management plans
- Sanction policy
- Sanction log
- Audit log review procedures
- Review logs and findings
- Corrective action plans

7.6.2 6.2 Retention

Retention Period: [TODO: 6 years from creation or last effective date]

Storage Location: [TODO: Document management system location]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 8

Workforce Security

Document ID: HIPAA-0110
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

8.1 1. Purpose

This document describes the Workforce Security procedures for AdminSend GmbH to ensure that all workforce members have appropriate access to ePHI and to prevent unauthorized access.

8.1.1 1.1 HIPAA Requirement

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

Implementation Specifications: - §164.308(a)(3)(ii)(A) - Authorization and/or Supervision (Addressable) - §164.308(a)(3)(ii)(B) - Workforce Clearance Procedure (Addressable) - §164.308(a)(3)(ii)(C) - Termination Procedures (Addressable)

8.2 2. Authorization and Supervision

8.2.1 2.1 Access Authorization

Principle: Access to ePHI is granted based on role, job function, and minimum necessary standard.

Authorization Process: 1. **Job Analysis:** Determine ePHI access requirements for role 2. **Access Request:** Manager submits access request 3. **Justification:** Document business need 4. **Approval:** Privacy Officer and/or Security Officer approve 5. **Provisioning:** IT provisions access 6. **Documentation:** Access logged 7. **Acknowledgment:** Employee acknowledges responsibilities

Authorization Criteria: - Job role requires ePHI access - Minimum necessary access only - Appropriate training completed - Background check completed (if required) - Confidentiality agreement signed

8.2.2 2.2 Supervision Requirements

Supervised Access: Workforce members with limited training or temporary status may require supervision when accessing ePHI.

Supervision Levels: | Workforce Type | Supervision Required | Supervisor | Duration | |———————-|———————|———————|———————-| | New employees (< 90 days) | Yes | Direct manager | Until training complete | | Temporary staff | Yes | Assigned supervisor | Duration of assignment | | Interns/students | Yes | Preceptor/instructor | Duration of program | | Contractors (short-term) | Yes | Project manager | Duration of contract |

Supervisor Responsibilities: - Monitor workforce member's ePHI access - Ensure compliance with policies - Provide guidance and training - Report violations - Document supervision activities

8.3 3. Workforce Clearance Procedure

8.3.1 3.1 Pre-Employment Screening

Background Check Requirements:

All Workforce with ePHI Access: - Identity verification - Employment history verification (7 years) - Education verification - Professional license verification (if applicable)

Workforce with Elevated Access: - Criminal background check - Credit check (for financial roles) - Reference checks (minimum 3)

Background Check Process: 1. **Conditional Offer:** Offer contingent on background check 2. **Authorization:** Candidate authorizes background check 3. **Screening:** Third-party vendor conducts check 4. **Review:** HR reviews results 5. **Decision:** Hire/no-hire decision 6. **Documentation:** Results documented and secured 7. **Adverse Action:** Follow FCRA requirements if adverse action taken

Background Check Vendor: [TODO: Vendor name]

8.3.2 3.2 Clearance Levels

Clearance Level	Requirements	Roles	ePHI Access
Level 1 - Basic	Identity verification, employment history	Administrative staff	Limited ePHI
Level 2 - Standard	Level 1 + education verification	Clinical staff	Full ePHI for patient care
Level 3 - Elevated	Level 2 + criminal background check	IT staff, billing	System-level ePHI access
Level 4 - Executive	Level 3 + credit check, references	Executives, compliance	All ePHI

8.3.3 3.3 Ongoing Clearance

Periodic Re-screening: - **Frequency:** [TODO: Every 3-5 years or as required by role] - **Scope:** Criminal background check, license verification - **Trigger Events:** Promotion, role change, security incident

Continuous Monitoring: - Professional license status - Sanctions or disciplinary actions - Criminal convictions (if permitted by law)

8.4 4. Termination Procedures

8.4.1 4.1 Termination Process

Termination Types: - Voluntary resignation - Involuntary termination - Retirement - End of contract/temporary assignment - Death

Termination Checklist:

Immediate Actions (Day of Termination): - [ ] Disable all system access (within 1 hour of notification) - [ ] Disable email account - [ ] Disable VPN access - [ ] Disable physical access (badge, keys) - [ ] Collect company devices (laptop, phone, tablet) - [ ] Collect access badges and keys - [ ] Change shared passwords/codes known to employee - [ ] Notify IT, Security, and Facilities

Within 24 Hours: - [ ] Review and archive employee's files - [ ] Forward email to manager (if appropriate) - [ ] Remove from distribution lists - [ ] Update organizational charts - [ ] Notify relevant departments - [ ] Document termination in HR system

Within 1 Week: - [ ] Conduct exit interview - [ ] Remind of confidentiality obligations - [ ] Collect signed acknowledgment of obligations - [ ] Final paycheck processing - [ ] COBRA notification (if applicable) - [ ] Return of property verification

8.4.2 4.2 Access Termination

System Access Termination: | System | Termination Method | Responsible | Verification | |———-|——————-|————-|————–| | Active Directory | Account disabled | IT | Automated report | | EHR System | User deactivated | IT | Manual verification | | Email | Mailbox disabled | IT | Automated report | | VPN | Certificate revoked | IT | Manual verification | | Physical Access | Badge deactivated | Facilities | Access log review |

Termination Verification: - IT generates termination report - Security Officer reviews report - Exceptions investigated and resolved - Documentation retained

8.4.3 4.3 Knowledge Transfer

Knowledge Transfer Process: 1. **Identification:** Identify critical knowledge and responsibilities 2. **Documentation:** Document processes and procedures 3. **Training:** Train replacement or team members 4. **Transition:** Gradual transition of responsibilities (if possible) 5. **Verification:** Verify knowledge transfer complete

Critical Knowledge Areas: - System access and passwords - Ongoing projects - Key contacts - Pending issues - Documentation locations

8.4.4 4.4 Post-Termination Monitoring

Monitoring Activities: - Review audit logs for terminated employee accounts - Monitor for unauthorized access attempts - Review for data exfiltration - Monitor for policy violations prior to termination

Monitoring Period: [TODO: 90 days post-termination]

8.5 5. Role-Based Access Control (RBAC)

8.5.1 5.1 Role Definitions

Role ID	Role Name	Department	ePHI Access Level	Systems	Approval Required
[TODO: ROLE-001]	Physician	Clinical	Full patient care	EHR, Lab, Imaging	Medical Director
[TODO: ROLE-002]	Nurse	Clinical	Full patient care	EHR, Medication	Nurse Manager
[TODO: ROLE-003]	Medical Assistant	Clinical	Limited	EHR (vitals, scheduling)	Clinical Manager
[TODO: ROLE-004]	Billing Specialist	Billing	Billing data only	Billing system	Billing Manager
[TODO: ROLE-005]	IT Administrator	IT	System admin	All systems	IT Manager + Security Officer
[TODO: ROLE-006]	Receptionist	Front Desk	Demographics only	EHR (scheduling)	Office Manager

8.5.2 5.2 Access Matrix

Role	Patient Demographics	Clinical Notes	Lab Results	Medications	Billing	System Admin
Physician	Read/Write	Read/Write	Read/Write	Read/Write	Read	No
Nurse	Read/Write	Read/Write	Read	Read/Write	No	No
Medical Assistant	Read/Write	Read	Read	No	No	No
Billing Specialist	Read	No	No	No	Read/Write	No

Role	Patient Demographics	Clinical Notes	Lab Results	Medications	Billing	System Admin
IT Administrator	No*	No*	No*	No*	No*	Yes
Receptionist	Read/Write	No	No	No	No	No

*IT Administrators have technical access but should not access ePHI unless required for troubleshooting

8.6 6. Training Requirements

8.6.1 6.1 Workforce Security Training

Initial Training (Within 30 days of hire): - HIPAA overview - Workforce security policies - Access control procedures - Password requirements - Confidentiality obligations - Sanctions for violations

Annual Training: - Workforce security refresher - Policy updates - Case studies - Emerging threats

Role-Specific Training: - Supervisors: Supervision responsibilities - IT Staff: Technical safeguards - Managers: Access authorization procedures

8.6.2 6.2 Training Documentation

Required Documentation: - Training attendance records - Training materials - Test scores (if applicable) - Acknowledgment of understanding - Training certificates

Retention: [TODO: 6 years]

8.7 7. Confidentiality Agreements

8.7.1 7.1 Confidentiality Agreement Requirements

All Workforce Members Must Sign: - Confidentiality agreement - Acceptable use policy - HIPAA acknowledgment - Security policy acknowledgment

Timing: - Before access to ePHI granted - Upon policy changes (re-acknowledgment) - Annually (re-acknowledgment)

8.7.2 7.2 Agreement Content

Confidentiality Agreement Must Include: - Obligation to protect PHI/ePHI - Prohibition on unauthorized access - Prohibition on unauthorized disclosure - Reporting requirements for incidents - Sanctions for violations - Obligations continue after termination - Acknowledgment of understanding

Agreement Storage: [TODO: HR personnel files, electronic repository]

8.8 8. Monitoring and Compliance

8.8.1 8.1 Workforce Security Monitoring

Monitoring Activities: - Access log reviews - Inappropriate access investigations - Policy compliance audits - Training completion tracking - Background check compliance - Termination procedure compliance

Monitoring Frequency: | Activity | Frequency | Responsible | |———-|———–|————-| | Access log review | Monthly | Security Officer | | Training compliance | Quarterly | HR + Privacy Officer | | Background check compliance | Annual | HR | | Termination procedure audit | Quarterly | Security Officer |

8.8.2 8.2 Compliance Metrics

Metric	Target	Current	Status
Training completion rate	100%	[TODO: %]	[TODO: Green/Yellow/Red]
Background checks completed	100%	[TODO: %]	[TODO: Green/Yellow/Red]
Termination procedures followed	100%	[TODO: %]	[TODO: Green/Yellow/Red]
Access reviews completed	100%	[TODO: %]	[TODO: Green/Yellow/Red]

8.9 9. Documentation and Records

8.9.1 9.1 Required Documentation

- Access authorization forms
- Background check results
- Confidentiality agreements
- Training records
- Termination checklists
- Access termination verification
- Supervision logs
- Incident reports

8.9.2 9.2 Retention

Retention Period: [TODO: 6 years from termination of employment or last effective date]

Storage Location: [TODO: HR system, document management system]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 9

Facility Access Controls

Document ID: HIPAA-0300
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

9.1 1. Purpose

This document describes the Facility Access Controls for AdminSend GmbH to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring properly authorized access is allowed.

9.1.1 1.1 HIPAA Requirement

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

Implementation Specifications: - §164.310(a)(2)(i) - Contingency Operations (Addressable) - §164.310(a)(2)(ii) - Facility Security Plan (Addressable) - §164.310(a)(2)(iii) - Access Control and Validation Procedures (Addressable) - §164.310(a)(2)(iv) - Maintenance Records (Addressable)

9.2 2. Facility Inventory

9.2.1 2.1 Facilities with ePHI

Facility ID	Facility Name	Address	Type	ePHI Systems	Access Level
[TODO: FAC-001]	Main Data Center	[TODO: Address]	Data Center	All production systems	Restricted

Facility ID	Facility Name	Address	Type	ePHI Systems	Access Level
[TODO: FAC-002]	Main Clinic	[TODO: Address]	Clinical	EHR workstations	Controlled
[TODO: FAC-003]	Administrative Office	[TODO: Address]	Office	Billing systems	Controlled
[TODO: FAC-004]	Backup Site	[TODO: Address]	DR Site	Backup systems	Restricted

9.2.2 2.2 Facility Classification

Restricted Access: - Data centers - Server rooms - Network equipment rooms - Backup storage areas

Controlled Access: - Clinical areas - Administrative offices - Medical records rooms

Public Access: - Waiting rooms - Public corridors - Cafeteria

9.3 3. Contingency Operations

9.3.1 3.1 Emergency Access Procedures

Purpose: Establish procedures to allow facility access in support of restoration of lost data under the disaster recovery and emergency mode operations plan.

Emergency Scenarios: - Fire or natural disaster - Power failure - System failure requiring immediate access - Security incident requiring investigation

Emergency Access Process: 1. **Authorization:** Security Officer or designee authorizes emergency access 2. **Escort:** Emergency personnel escorted by authorized staff 3. **Documentation:** All emergency access logged 4. **Restoration:** Normal access controls restored after emergency 5. **Review:** Post-incident review of emergency access

Emergency Contacts: | Role | Name | Phone (24/7) | Backup | |——|——|————|——— | | Security Officer | {{ meta.roles.security_officer.name }} | [TODO: Phone] | [TODO: Backup name/phone] | | Facility Manager | [TODO: Name] | [TODO: Phone] | [TODO: Backup] | | IT Manager | [TODO: Name] | [TODO: Phone] | [TODO: Backup] |

9.3.2 3.2 Emergency Access Equipment

Emergency Access Tools: - Master keys (secured in break-glass box) - Access cards (emergency override) - Lock bypass tools (authorized personnel only) - Emergency lighting - Communication devices

Storage Location: [TODO: Secure location with documented access]

9.4 4. Facility Security Plan

9.4.1 4.1 Physical Security Measures

Perimeter Security: - Fencing: [TODO: Yes/No, Description] - Gates: [TODO: Yes/No, Description] - Lighting: [TODO: Description] - Signage: [TODO: “Authorized Personnel Only” signs]

- Landscaping: [TODO: Clear sight lines]

Building Security: - Exterior doors: [TODO: Number, locking mechanisms] - Windows: [TODO: Security measures] - Loading docks: [TODO: Security measures] - Roof access: [TODO: Security measures]

Interior Security: - Reception/Security desk: [TODO: Yes/No, Hours] - Security guards: [TODO: Yes/No, Schedule] - Visitor management: [TODO: System/Process] - Escort requirements: [TODO: Areas requiring escort]

Data Center/Server Room Security: - Dedicated room: [TODO: Yes/No] - Reinforced walls: [TODO: Yes/No] - Raised floor: [TODO: Yes/No] - Fire suppression: [TODO: Type] - Environmental monitoring: [TODO: Temperature, humidity] - Water detection: [TODO: Yes/No] - Backup power: [TODO: UPS, generator]

9.4.2 4.2 Access Control Systems

Physical Access Control System: - **System Type:** [TODO: Card reader, biometric, keypad] - **Vendor:** [TODO: Vendor name] - **Coverage:** [TODO: Doors/areas covered] - **Monitoring:** [TODO: 24/7 monitoring, alerts]

Access Control Features: - Individual identification - Time-based access restrictions - Area-based access restrictions - Anti-passback - Audit logging - Real-time alerts

Access Card Management: - Card issuance process - Card deactivation process - Lost/stolen card procedures - Card return upon termination

9.4.3 4.3 Surveillance Systems

Video Surveillance: - **Coverage:** [TODO: Entrances, exits, server rooms, etc.] - **Camera Type:** [TODO: Fixed, PTZ, resolution] - **Recording:** [TODO: Continuous, motion-activated] - **Retention:** [TODO: Days/months] - **Monitoring:** [TODO: Live monitoring, review schedule]

Surveillance Locations: | Location | Camera Count | Recording | Retention | Purpose | |———-|————|———|———|———| | [TODO: Main entrance] | [TODO: 2] | Continuous | [TODO: 90 days] | Access monitoring | | [TODO: Server room] | [TODO: 1] | Continuous | [TODO: 90 days] | Security monitoring | | [TODO: Parking lot] | [TODO: 4] | Motion | [TODO: 30 days] | Perimeter security |

9.5 5. Access Control and Validation Procedures

9.5.1 5.1 Access Authorization

Authorization Process: 1. **Request:** Manager submits access request 2. **Justification:** Business need documented 3. **Approval:** Security Officer approves 4. **Provisioning:** Facility Manager provisions access 5. **Documentation:** Access logged in system 6. **Notification:** Employee notified of access granted

Access Levels: | Level | Description | Authorization Required | Areas Accessible | |——-|————-|———————|————| | Level 1 - Public | General public | None | Waiting areas, public corridors | | Level 2 - Employee | Regular employees | Manager approval | Office areas, break rooms | | Level 3 - Clinical | Clinical staff | Manager + Privacy Officer | Clinical areas, medical records | |

Level 4 - IT | IT staff | IT Manager + Security Officer | Server rooms, network closets | | Level 5 - Executive | Executive access | CEO approval | All areas |

9.5.2 5.2 Visitor Management

Visitor Procedures: 1. **Check-in:** Visitor checks in at reception 2. **Identification:** Photo ID required and recorded 3. **Badge:** Visitor badge issued 4. **Escort:** Visitor escorted at all times in restricted areas 5. **Log:** Visit logged (name, company, purpose, time in/out, host) 6. **Check-out:** Visitor returns badge and checks out

Visitor Types: - Vendors/contractors - Business associates - Auditors - Guests - Delivery personnel

Visitor Badge: Clearly marked "VISITOR" badge, different color from employee badges

9.5.3 5.3 Access Validation

Access Review Process: - **Frequency:** Quarterly - **Reviewer:** Facility Manager + Security Officer - **Scope:** All active access permissions - **Actions:** Revoke unnecessary access, update records

Access Validation Checklist: - [ ] Verify employee still requires access - [ ] Verify access level appropriate for role - [ ] Verify no terminated employees have active access - [ ] Verify no expired temporary access - [ ] Update access documentation

9.5.4 5.4 Access Termination

Termination Process: 1. **Notification:** HR notifies Facility Manager and Security Officer 2. **Immediate Revocation:** Access revoked immediately upon termination 3. **Badge Collection:** Employee badge collected 4. **Key Collection:** All keys collected 5. **Verification:** Access termination verified in system 6. **Documentation:** Termination logged

Termination Checklist: - [ ] Access card deactivated - [ ] Keys returned - [ ] Alarm codes changed (if applicable) - [ ] Visitor escort privileges revoked - [ ] Documentation updated

9.6 6. Maintenance Records

9.6.1 6.1 Facility Maintenance

Maintenance Activities: - Access control system maintenance - Surveillance system maintenance - Lock and key maintenance - Alarm system maintenance - Fire suppression system maintenance - Environmental controls maintenance - Emergency lighting maintenance

Maintenance Schedule: | System | Maintenance Type | Frequency | Vendor | Last Service | Next Service | |———|———————|————|———|———————|———————| | [TODO: Access control] | Preventive | Quarterly | [TODO: Vendor] | [TODO: Date] | [TODO: Date] | | [TODO: Surveillance] | Preventive | Semi-annual | [TODO: Vendor] | [TODO: Date] | [TODO: Date] | | [TODO: Fire suppression] | Inspection | Annual | [TODO: Vendor] | [TODO: Date] | [TODO: Date] |

9.6.2 6.2 Maintenance Documentation

Required Documentation: - Maintenance work orders - Service reports - Parts replaced - System tests performed - Technician credentials - Access logs for maintenance personnel

Retention: [TODO: 6 years]

9.6.3 6.3 Maintenance Access Control

Vendor Access: - Vendor escorted during maintenance - Vendor access logged - Vendor credentials verified - Background checks for regular vendors - Business Associate Agreement (if PHI access possible)

9.7 7. Physical Security Incidents

9.7.1 7.1 Incident Types

- Unauthorized facility access
- Tailgating
- Lost/stolen access cards or keys
- Forced entry
- Surveillance system tampering
- Alarm system failures

9.7.2 7.2 Incident Response

Response Process: 1. **Detection:** Incident detected (alarm, observation, report) 2. **Notification:** Security Officer notified immediately 3. **Assessment:** Assess severity and impact 4. **Containment:** Secure area, change access codes if needed 5. **Investigation:** Review logs, surveillance footage 6. **Remediation:** Implement corrective actions 7. **Documentation:** Document incident and response 8. **Review:** Post-incident review and lessons learned

9.7.3 7.3 Incident Log

Incident ID	Date	Type	Location	Description	Response	Status
[TODO: INC-001]	[TODO: Date]	[TODO: Type]	[TODO: Location]	[TODO: Description]	[TODO: Actions taken]	[TODO: Closed]

9.8 8. Documentation and Records

9.8.1 8.1 Required Documentation

- Facility security plan
- Access authorization records
- Visitor logs
- Access review records
- Maintenance records
- Incident reports
- Surveillance footage (per retention policy)

9.8.2 8.2 Retention

Retention Period: [TODO: 6 years from creation or last effective date]

Storage Location: [TODO: Document management system location]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 10

Workstation Use and Security

Document ID: HIPAA-0310
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

10.1 1. Purpose

This document describes the Workstation Use and Workstation Security policies for AdminSend GmbH to specify proper functions to be performed, the manner in which those functions are to be performed, and physical attributes of the surroundings of workstations that access ePHI.

10.1.1 1.1 HIPAA Requirements

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

10.2 2. Workstation Use

10.2.1 2.1 Workstation Definition

Workstation: An electronic computing device (e.g., laptop, desktop computer, tablet, smartphone) and its electronic media used to access, create, receive, maintain, or transmit ePHI.

Workstation Types: - Desktop computers - Laptop computers - Tablets - Smartphones - Thin clients - Workstations on wheels (WOWs) - Kiosks

10.2.2 2.2 Authorized Use

Permitted Uses: - Accessing ePHI for treatment, payment, or healthcare operations - Creating and maintaining patient records - Communicating with patients and healthcare team - Billing and administrative functions - Authorized research activities

Prohibited Uses: - Personal use (except minimal incidental use) - Accessing ePHI without authorization - Sharing login credentials - Installing unauthorized software - Connecting unauthorized devices - Accessing inappropriate websites - Downloading unauthorized files

10.2.3 2.3 User Responsibilities

Workforce Members Must: - Use workstations only for authorized purposes - Protect login credentials - Lock workstation when leaving (even briefly) - Log off when finished - Report lost, stolen, or compromised workstations immediately - Keep workstation software updated - Not share workstations without proper logout/login - Position screens to prevent unauthorized viewing - Use privacy screens in public areas

10.3 3. Workstation Security

10.3.1 3.1 Physical Security

Workstation Placement: - Position to minimize unauthorized viewing - Avoid placement near windows or public areas - Ensure adequate physical security of location - Consider traffic patterns and visibility

Physical Security Controls: - Cable locks for laptops - Locked offices or secured areas - Privacy screens/filters - Automatic screen locks - Physical barriers (walls, partitions)

Mobile Workstations: - Laptop bags that don't identify contents - Never leave unattended in vehicles - Use hotel safes when traveling - Encrypt all mobile devices - Enable remote wipe capability

10.3.2 3.2 Technical Security

Authentication: - Unique user ID required - Strong password or biometric authentication - Multi-factor authentication (for remote access) - No shared accounts

Automatic Logoff/Lock: - Screen lock after [TODO: 5-15] minutes of inactivity - Automatic logoff after [TODO: 30] minutes of inactivity - Require re-authentication to resume

Encryption: - Full disk encryption required for all workstations - Encryption standard: [TODO: AES-256 or equivalent] - Encryption key management procedures

Antivirus/Anti-malware: - Endpoint protection software required - Real-time scanning enabled - Automatic updates enabled - Regular scans scheduled

Firewall: - Host-based firewall enabled - Default deny inbound connections - Only authorized applications allowed

Software Updates: - Operating system patches applied within [TODO: 30] days - Critical security patches applied within [TODO: 7] days - Application updates applied per vendor recommendations

10.3.3 3.3 Configuration Standards

Baseline Configuration: - Approved operating system version - Approved applications only - Unnecessary services disabled - Default passwords changed - Administrative rights restricted - Audit logging enabled

Configuration Management: - Standard images for workstation deployment - Configuration changes documented and approved - Regular configuration audits - Non-compliant workstations remediated

10.4 4. Workstation Inventory

10.4.1 4.1 Asset Inventory

Asset ID	Type	Location	User	ePHI Access	Encryption	Last Update
[TODO: WS-001]	Desktop	[TODO: Office 101]	[TODO: User name]	Yes	Yes	[TODO: Date]
[TODO: WS-002]	Laptop	[TODO: Mobile]	[TODO: User name]	Yes	Yes	[TODO: Date]
[TODO: WS-003]	Tablet	[TODO: Clinic A]	[TODO: Shared]	Yes	Yes	[TODO: Date]

10.4.2 4.2 Asset Tracking

Tracking Requirements: - Asset tag/ID - Serial number - Make and model - Assigned user - Location - ePHI access (Yes/No) - Encryption status - Last security update - Warranty/support expiration

Inventory Updates: - New workstation deployment - Workstation reassignment - Workstation retirement - Location changes - Quarterly inventory verification

10.5 5. Workstation Lifecycle

10.5.1 5.1 Procurement

Procurement Requirements: - Meet minimum security standards - Compatible with security software - Support full disk encryption - Approved by IT department - Include appropriate warranty/support

Approval Process: 1. Department submits request 2. IT reviews technical requirements 3. Security Officer approves security features 4. Procurement processes order

10.5.2 5.2 Deployment

Deployment Process: 1. **Imaging:** Install standard image 2. **Configuration:** Apply security configuration 3. **Encryption:** Enable full disk encryption 4. **Software:** Install required applications 5. **Testing:** Verify functionality and security 6. **Documentation:** Add to asset inventory

7. **Assignment:** Assign to user 8. **Training:** Provide user training 9. **Acknowledgment:** User signs acceptable use agreement

10.5.3 5.3 Maintenance

Maintenance Activities: - Software updates and patches - Antivirus updates - Hardware repairs - Performance optimization - Security scans

Maintenance Schedule: | Activity | Frequency | Responsible | |———-|———–|————-| | OS patches | Monthly | IT | | Antivirus updates | Daily (automatic) | Endpoint protection | | Security scans | Weekly | IT Security | | Hardware inspection | Annual | IT |

10.5.4 5.4 Retirement/Disposal

Retirement Process: 1. **Decommission:** Remove from production 2. **Data Sanitization:** Securely wipe all data 3. **Verification:** Verify data destruction 4. **Documentation:** Document disposal 5. **Physical Destruction:** Destroy storage media (if required) 6. **Certificate:** Obtain certificate of destruction 7. **Inventory Update:** Remove from asset inventory

Data Sanitization Methods: - Software-based wiping (NIST 800-88 compliant) - Degaussing (for magnetic media) - Physical destruction (shredding, crushing)

Sanitization Standards: - Minimum 3-pass overwrite - Verification of sanitization - Documentation of method used - Certificate of destruction retained

10.6 6. Remote Access Workstations

10.6.1 6.1 Remote Access Requirements

Remote Access Scenarios: - Work from home - Telehealth - Mobile clinicians - Business travel - Emergency access

Security Requirements: - VPN required for all remote access - Multi-factor authentication required - Encrypted connections only - Company-owned or approved devices only - Compliance with all workstation security policies

10.6.2 6.2 Home Office Security

Home Office Requirements: - Dedicated workspace (if possible) - Physical security (locked room/area) - Secure Wi-Fi (WPA3 or WPA2) - No shared computer use - Privacy from family members - Secure document storage

Home Network Security: - Change default router password - Enable router firewall - Disable WPS - Use strong Wi-Fi password - Keep router firmware updated - Separate guest network

10.7 7. Shared Workstations

10.7.1 7.1 Shared Workstation Policy

Shared Workstation Scenarios: - Clinical workstations on wheels (WOWs) - Nurse station computers - Kiosks - Conference room computers

Security Requirements: - Individual login required (no shared accounts) - Automatic logoff after inactivity - Clear screen policy (log off between users) - Physical security of location - Regular cleaning and maintenance

10.7.2 7.2 Kiosk Mode

Kiosk Configuration: - Limited functionality - Restricted application access - No local data storage - Automatic session timeout - Automatic return to login screen - Tamper-resistant hardware

10.8 8. Mobile Device Management (MDM)

10.8.1 8.1 MDM Requirements

MDM Capabilities: - Remote wipe - Encryption enforcement - Password policy enforcement - Application management - Device compliance monitoring - Location tracking (if permitted)

MDM Enrollment: - All mobile devices with ePHI access must be enrolled - Enrollment before ePHI access granted - User acknowledgment of MDM capabilities

10.8.2 8.2 BYOD (Bring Your Own Device)

BYOD Policy: [TODO: Allowed/Not Allowed]

If BYOD allowed: - MDM enrollment required - Containerization of work data - Separate work/personal data - Remote wipe of work data only - User agreement acknowledging MDM - Compliance with all security policies

10.9 9. Incident Response

10.9.1 9.1 Workstation Incidents

Incident Types: - Lost or stolen workstation - Malware infection - Unauthorized access - Physical damage - Data breach - Policy violation

10.9.2 9.2 Reporting Procedures

Immediate Reporting Required: 1. **Report:** Immediately report to IT Help Desk and Security Officer 2. **Disable:** IT disables remote access and network access 3. **Assess:** Security Officer assesses incident 4. **Contain:** Contain incident (remote wipe if necessary) 5. **Investigate:** Investigate scope and impact 6. **Remediate:** Implement corrective actions 7. **Document:** Document incident and response 8. **Follow-up:** Conduct post-incident review

Contact Information: - IT Help Desk: [TODO: Phone/Email] - Security Officer: {{ meta.roles.security_officer.email }} - After Hours: [TODO: Emergency contact]

10.10 10. Training and Awareness

10.10.1 10.1 Training Requirements

Initial Training: - Workstation use policy - Workstation security requirements - Physical security measures - Incident reporting - Acceptable use policy

Annual Training: - Policy refresher - Emerging threats - Best practices - Case studies

Just-in-Time Training: - New workstation deployment - Policy changes - After security incidents

10.10.2 10.2 Awareness Activities

- Security reminders (email, posters)
- Screen lock reminders
- Clean desk policy reminders
- Phishing awareness
- Social engineering awareness

10.11 11. Monitoring and Compliance

10.11.1 11.1 Compliance Monitoring

Monitoring Activities: - Workstation configuration audits - Encryption compliance checks - Software update compliance - Antivirus status checks - Physical security inspections - Policy compliance audits

Monitoring Frequency: | Activity | Frequency | Responsible | |———-|———–|————-| | Configuration audit | Quarterly | IT Security | | Encryption check | Monthly | IT Security | | Update compliance | Weekly | IT | | Physical inspection | Semi-annual | Facilities + IT |

10.11.2 11.2 Non-Compliance

Non-Compliance Actions: 1. **Identification:** Non-compliant workstation identified 2. **Notification:** User notified 3. **Remediation:** User given timeframe to remediate 4. **Escalation:** Escalate if not remediated 5. **Restriction:** Restrict ePHI access if necessary 6. **Sanctions:** Apply sanctions per policy

10.12 12. Documentation and Records

10.12.1 12.1 Required Documentation

- Workstation inventory
- Configuration standards
- Deployment records
- Maintenance records
- Disposal/sanitization certificates
- Incident reports
- Training records
- Compliance audit results

10.12.2 12.2 Retention

Retention Period: [TODO: 6 years from retirement/disposal]

Storage Location: [TODO: Asset management system, document repository]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 11

Access Control

Document ID: HIPAA-0400
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

11.1 1. Purpose

This document describes the Access Control technical safeguards for AdminSend GmbH to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to authorized persons or software programs.

11.1.1 1.1 HIPAA Requirement

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

Implementation Specifications: - §164.312(a)(2)(i) - Unique User Identification (Required) - §164.312(a)(2)(ii) - Emergency Access Procedure (Required) - §164.312(a)(2)(iii) - Automatic Logoff (Addressable) - §164.312(a)(2)(iv) - Encryption and Decryption (Addressable)

11.2 2. Unique User Identification

11.2.1 2.1 User ID Requirements

Requirement: Assign a unique name and/or number for identifying and tracking user identity.

User ID Standards: - Unique to each individual user - Not shared between users - Not reused after termination - Format: [TODO: firstname.lastname, employee ID, etc.] - Minimum length: [TODO: 6 characters]

Prohibited Practices: - Shared accounts - Generic accounts (except for specific approved purposes) - Default accounts (must be disabled or renamed) - Guest accounts (must be disabled)

11.2.2 2.2 User Account Management

Account Creation Process: 1. Manager submits access request 2. HR verifies employment status 3. Security Officer approves based on role 4. IT creates unique user account 5. User notified of account creation 6. User completes initial login and password setup

Account Types: | Account Type | Purpose | Approval Required | Monitoring | |————–|————————–|————————-|————–| | Standard User | Regular workforce member | Manager | Standard | | Privileged User | System administration | IT Manager + Security Officer | Enhanced | | Service Account | Automated processes | Security Officer | Enhanced | | Emergency Access | Break-glass access | Security Officer | Immediate review |

11.2.3 2.3 Authentication Methods

Primary Authentication: - Username and password - Minimum password requirements: - Length: [TODO: 12 characters minimum] - Complexity: Upper, lower, number, special character - History: [TODO: 12 previous passwords remembered] - Age: Maximum [TODO: 90 days], minimum [TODO: 1 day] - Lockout: [TODO: 5 failed attempts], lockout duration [TODO: 30 minutes]

Multi-Factor Authentication (MFA): - Required for: Remote access, privileged accounts, ePHI access from untrusted networks - Methods: SMS code, authenticator app, hardware token, biometric - Backup codes provided for MFA recovery

Single Sign-On (SSO): - Centralized authentication - Reduces password fatigue - Audit trail of access - Integration with MFA

11.3 3. Emergency Access Procedure

11.3.1 3.1 Emergency Access Definition

Emergency Situations: - System failure preventing normal authentication - Natural disaster - Cyberattack requiring immediate response - Life-threatening patient situation requiring immediate ePHI access - Critical system maintenance

11.3.2 3.2 Break-Glass Accounts

Break-Glass Account Characteristics: - Highly privileged access - Used only in emergencies - Credentials secured (sealed envelope, password vault) - Immediate notification upon use - Automatic logging of all activities - Immediate review required

Break-Glass Account Inventory: | Account ID | System | Access Level | Credential Location | Last Used | Reviewed By | |————–|——–|————–|———————|————–|————–| | [TODO: BG-001] | Active Directory | Domain Admin | [TODO: Secure vault] | [TODO: Date] | [TODO: Security Officer] | | [TODO: BG-002] | EHR System | System Admin | [TODO: Secure vault] | [TODO: Date] | [TODO: Security Officer] |

11.3.3 3.3 Emergency Access Process

Process Steps: 1. **Determination:** Determine emergency situation exists 2. **Authorization:** Security Officer or designee authorizes emergency access 3. **Access:** Use break-glass credentials 4. **Logging:** All activities automatically logged 5. **Notification:** Security Officer immediately notified 6. **Monitoring:** Real-time monitoring of emergency access activities 7. **Review:** Immediate post-access review 8. **Documentation:** Document emergency, actions taken, justification 9. **Credential Rotation:** Change break-glass credentials after use

Emergency Access Log: | Date/Time | User | System | Reason | Authorized By | Actions Taken | Review Date | |————|——|——|——|————|————|————-| | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

11.4 4. Automatic Logoff

11.4.1 4.1 Automatic Logoff Requirements

Requirement: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Rationale: Prevent unauthorized access to ePHI when workstation left unattended.

11.4.2 4.2 Timeout Settings

Inactivity Timeouts: | System/Application | Timeout Period | Action | Override Allowed | |————————|————-|——|————| | Workstations | [TODO: 15 minutes] | Screen lock | No | | EHR System | [TODO: 10 minutes] | Session timeout | No | | Web Applications | [TODO: 20 minutes] | Session timeout | No | | VPN | [TODO: 30 minutes] | Disconnect | No | | Mobile Devices | [TODO: 5 minutes] | Screen lock | No |

Timeout Actions: - **Screen Lock:** Requires password to unlock, session remains active - **Session Timeout:** Terminates session, requires re-authentication - **Disconnect:** Terminates network connection

11.4.3 4.3 Implementation

Technical Implementation: - Group Policy (Windows) - Configuration profiles (macOS, iOS) - Application-level timeouts - Network-level timeouts (VPN, firewall)

User Notification: - Warning before timeout (e.g., 2 minutes) - Clear indication of locked state - Instructions for unlocking

11.5 5. Encryption and Decryption

11.5.1 5.1 Encryption Requirements

Requirement: Implement a mechanism to encrypt and decrypt ePHI.

Encryption Use Cases: - ePHI at rest (stored data) - ePHI in transit (transmitted data) - Backup media - Mobile devices - Removable media - Email containing ePHI

11.5.2 5.2 Encryption Standards

Approved Encryption Algorithms: - **Symmetric:** AES-256, AES-128 - **Asymmetric:** RSA-2048 or higher, ECC - **Hashing:** SHA-256, SHA-512 - **TLS:** TLS 1.2 or higher

Prohibited Algorithms: - DES, 3DES - MD5, SHA-1 - SSL, TLS 1.0, TLS 1.1 - RC4

11.5.3 5.3 Encryption at Rest

Full Disk Encryption: - All workstations and laptops: [TODO: BitLocker, FileVault, LUKS] - All servers with ePHI: [TODO: BitLocker, dm-crypt] - All mobile devices: [TODO: Native device encryption]

Database Encryption: - Transparent Data Encryption (TDE) for databases - Column-level encryption for sensitive fields - Encryption key management

File/Folder Encryption: - Encrypted file systems - Encrypted containers - Document-level encryption

11.5.4 5.4 Encryption in Transit

Network Encryption: - TLS 1.2+ for all web traffic - VPN for remote access (IPsec, SSL VPN) - Encrypted email (S/MIME, PGP) - SFTP/SCP for file transfers (no FTP) - HTTPS for all web applications

Wireless Encryption: - WPA3 or WPA2-Enterprise - No WEP or open networks - Certificate-based authentication

11.5.5 5.5 Key Management

Key Management Lifecycle: 1. **Generation:** Cryptographically secure random generation 2. **Distribution:** Secure key distribution mechanisms 3. **Storage:** Hardware Security Module (HSM) or secure key vault 4. **Rotation:** Regular key rotation schedule 5. **Backup:** Secure backup of encryption keys 6. **Destruction:** Secure destruction when no longer needed

Key Management System: - Centralized key management - Access controls on keys - Audit logging of key access - Key escrow/recovery procedures

Key Rotation Schedule: | Key Type | Rotation Frequency | Responsible | |———-|———————-|————-| | Disk encryption keys | [TODO: Annually] | IT Security | | Database encryption keys | [TODO: Annually] | Database Admin | | TLS certificates | [TODO: Annually or per vendor] | IT Security | | VPN keys | [TODO: Quarterly] | Network Admin |

11.6 6. Access Control Lists (ACLs)

11.6.1 6.1 ACL Management

ACL Principles: - Least privilege - Need-to-know - Separation of duties - Defense in depth

ACL Components: - User/group identity - Resource (file, folder, application, database) - Permissions (read, write, execute, delete) - Conditions (time, location, device)

11.6.2 6.2 Permission Levels

Standard Permission Levels: | Level | Description | Typical Roles | |——-|————-|————— | | No Access | No permissions | Default for all users | | Read | View only | Auditors, read-only users | | Read/Write | View and modify | Standard users | | Full Control | All permissions | Administrators, owners |

11.6.3 6.3 ACL Review

Review Process: - **Frequency:** Quarterly - **Scope:** All ePHI resources - **Reviewers:** Resource owners + Security Officer - **Actions:** Remove unnecessary permissions, update for role changes

11.7 7. Privileged Access Management (PAM)

11.7.1 7.1 Privileged Account Definition

Privileged Accounts: - System administrators - Database administrators - Network administrators - Application administrators - Security administrators

Privileged Access Characteristics: - Elevated permissions - Access to sensitive systems - Ability to modify security controls - Access to all ePHI

11.7.2 7.2 PAM Controls

PAM Requirements: - Separate privileged accounts from standard accounts - Just-in-time (JIT) privilege elevation - Session recording for privileged access - Enhanced monitoring and alerting - Regular access reviews - MFA required for privileged access

PAM Solution: [TODO: CyberArk, BeyondTrust, Thycotic, etc.]

11.8 8. Monitoring and Auditing

11.8.1 8.1 Access Monitoring

Monitoring Activities: - Failed login attempts - Successful logins (especially after hours) - Privileged account usage - Emergency access usage - Permission changes - Account creation/deletion - Password resets

Monitoring Tools: - SIEM (Security Information and Event Management) - Log aggregation and analysis - User behavior analytics (UBA) - Automated alerting

11.8.2 8.2 Access Auditing

Audit Activities: - User access reviews - Privileged access reviews - ACL reviews - Inactive account reviews - Orphaned account reviews

Audit Frequency: | Activity | Frequency | Responsible | |———-|————|————-| | User access review | Quarterly | Managers + Security Officer | | Privileged access review | Monthly | Security Officer | | ACL review | Quarterly | Resource owners | | Inactive account review | Monthly | IT + HR |

11.9 9. Documentation and Records

11.9.1 9.1 Required Documentation

- User account inventory
- Privileged account inventory
- Break-glass account procedures
- Emergency access logs
- Access review records
- ACL documentation
- Encryption key inventory
- Timeout configuration documentation

11.9.2 9.2 Retention

Retention Period: [TODO: 6 years from creation or last effective date]

Storage Location: [TODO: Identity management system, document repository]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default('') }}	{{ meta.document.author | default('') }}	Initial creation

ewpage

Chapter 12

Privacy Practices and Individual Rights

Document ID: HIPAA-0500
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

12.1 1. Purpose

This document describes the privacy practices and procedures for managing individual rights under the HIPAA Privacy Rule for AdminSend GmbH.

12.1.1 1.1 HIPAA Requirements

Privacy Rule Requirements: - Notice of Privacy Practices (§164.520) - Right of Access (§164.524) - Right to Amend (§164.526) - Accounting of Disclosures (§164.528) - Right to Request Restrictions (§164.522(a)) - Right to Confidential Communications (§164.522(b))

12.2 2. Notice of Privacy Practices

12.2.1 2.1 Notice Requirements

Content Requirements: - Uses and disclosures of PHI - Individual rights - Covered entity duties - Complaint procedures - Contact information - Effective date

Distribution: - First service delivery - Upon request - Posted prominently - Available on website - Material changes require new notice

[TODO: Additional sections for each individual right…]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 13

Breach Notification and Incident Response

Document ID: HIPAA-0600
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

13.1 1. Purpose

This document describes the breach notification and incident response procedures for AdminSend GmbH as required by the HIPAA Breach Notification Rule.

13.1.1 1.1 HIPAA Requirements

Breach Notification Rule (45 CFR §§ 164.400-164.414): - Breach definition and assessment - Notification to individuals - Notification to HHS - Notification to media (500+ individuals) - Business associate notification obligations

13.2 2. Breach Definition

Breach: Acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI.

Exceptions: - Unintentional acquisition/access by workforce in good faith - Inadvertent disclosure within organization - Disclosure where recipient couldn't reasonably retain information

13.2.1 2.1 Breach Risk Assessment

Risk Assessment Factors: 1. Nature and extent of PHI involved 2. Unauthorized person who used/received PHI 3. Whether PHI was actually acquired or viewed 4. Extent to which risk has been mitigated

[TODO: Additional sections for notification procedures…]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 14

Appendix: Risk Analysis Template

Document ID: HIPAA-0700
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

14.1 1. Purpose

This appendix provides a template for conducting HIPAA Security Rule risk analysis as required by §164.308(a)(1)(ii)(A).

14.2 2. Risk Analysis Template

14.2.1 2.1 Scope Definition

ePHI Inventory: | Data Element | Format | Storage Location | Access Controls | Encryption | |————|——|————|————|———| | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

14.2.2 2.2 Threat and Vulnerability Assessment

Threat	Vulnerability	Likelihood	Impact	Risk Level	Mitigation
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

14.2.3 2.3 Risk Treatment Plan

Risk ID	Treatment	Controls	Timeline	Owner	Status
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage