

IADDA HIPAA HANDBOOK
TABLE OF CONTENTS
BINDER 3

SECTION 1 Overview

SECTION 2 Organizational Requirements (OR)

Policy No. Policy Name

OR101	Definitions Attachment OR101A: Information System Components
OR102	Hybrid Entity
OR103	Affiliated Covered Entity
OR104	Overview of Covered Entity Responsibilities
OR105	Business Associate Agreement Attachment OR105A: Sample Business Associate Addendum to Existing Agreement Attachment OR105B: Sample Business Associate Agreement
OR106	Group Health Plan Amendment
OR107	Maintenance of Policies and Procedures
OR108	Documentation

SECTION 3 Policies for Administrative Safeguards (AS)

Standard 1: Security Management Process

Policy No. Policy Name

AS101	Risk Analysis (Required) Attachment AS101A: Risk Analysis Checklist Attachment AS101B: Risk Assessment Checklist
AS102	Risk Management (Required)
AS103	Sanctions (Required)
AS104	Information System Activity Review (Required) Attachment AS104A: Audit Log Guidelines

Standard 2: Assigned Security Responsibility

Policy No. Policy Name

- AS201 Responsibilities of Security Officer (Required)
Attachment AS201A: Sample Security Officer Job Description
- AS202 Specific Responsibilities of Covered Entity (Required)

Standard 3: Workforce Security

Policy No. Policy Name

- AS301 Authorization and/or Supervision of Workforce Members (Addressable)
- AS302 Clearance Procedures (Addressable)
- AS303 Termination Procedures (Addressable)
Attachment AS303A: Security Considerations for Termination
Attachment AS303B: Disabling Access After Termination Checklist

Standard 4: Information Access Management

Policy No. Policy Name

- AS401 Isolating Healthcare Clearinghouse Functions (Required)
- AS402 Access Authorization (Addressable)
- AS403 Access Establishment and Modification (Addressable)

Standard 5: Awareness and Training

Policy No. Policy Name

- AS501 Workforce Training (Required)
Attachment AS501A: Workforce Training Guidelines
Attachment AS501B: Training Do's and Don'ts
- AS502 Security Reminders (Addressable)
Attachment AS502A: Security Training Plan Concepts
Attachment AS502B: Security Reminders
- AS503 Protection from Malicious Software (Addressable)
- AS504 Log-in Monitoring (Addressable)
- AS505 Password Management (Addressable)

Standard 6: Security Incident Procedures

Policy No. Policy Name

AS601 Response and Reporting of Security Incidents (Required)

Attachment AS601A: Sample Security Incident Log

Attachment AS601B: Sample Security Violation/Incident Report

Standard 7: Contingency Plan

Policy No. Policy Name

AS701 Data Backup Plan (Required)

Attachment AS701A: Backup Plan Guidelines

AS702 Disaster Recovery Plan (Required)

AS703 Emergency Mode Operation Plan (Required)

AS704 Testing and Revision Procedure (Addressable)

AS705 Applications and Data Criticality Analysis (Addressable)

Standard 8: Evaluation

Policy No. Policy Name

AS801 Evaluation Format (Required)

Attachment AS801A: Periodic Evaluation Checklist for Security Policies and Procedures

SECTION 4 Policies for Physical Safeguards (PS)

Standard 1: Facility Access Controls

Policy No. Policy Name

PS101 Contingency Operations (Addressable)

Attachment PS101A: Contingency Operations Plan Components

PS102 Facility Security Plan (Addressable)

PS103 Access Control and Validation Procedures (Addressable)

Attachment PS103A: Access Control Tool

PS104 Maintenance Records (Addressable)

Standard 2: Workstation Use

Policy No.	Policy Name
------------	-------------

PS201	Workstation Use (Required)
-------	----------------------------

Attachment PS201A: E-Mail and Internet Use Guidelines

Standard 3: Workstation Security

Policy No.	Policy Name
------------	-------------

PS301	Workstation Security (Required)
-------	---------------------------------

Standard 4: Device and Media Controls
--

Policy No.	Policy Name
------------	-------------

PS401	Disposal (Required)
-------	---------------------

PS402	Media Re-Use (Required)
-------	-------------------------

PS403	Accountability (Addressable)
-------	------------------------------

PS404	Data Backup and Storage (Addressable)
-------	---------------------------------------

SECTION 5 Technical Safeguards (TS)

Standard 1: Access

Policy No.	Policy Name
------------	-------------

TS101	Unique User Identification (Required)
-------	---------------------------------------

TS102	Emergency Access Procedure (Required)
-------	---------------------------------------

TS103	Automatic Log off (Addressable)
-------	---------------------------------

TS104	Encryption and Decryption (Addressable)
-------	---

Standard 2: Audit Control

Policy No.	Policy Name
------------	-------------

TS201	Audit Controls (Required)
-------	---------------------------

Standard 3: Integrity

Policy No. Policy Name

TS301 Authentication of Electronic PHI (Addressable)

Standard 4: Authentication

Policy No. Policy Name

TS401 Authentication of Entity or Person (Required)

Standard 5: Transmission Security

Policy No. Policy Name

TS501 Integrity Controls (Addressable)

TS502 Encryption (Addressable)

SECTION 6 References

Security Standards

REF001 45 CFR Part 160
45 CFR Part 162
45 CFR Part 164

National Institute of Standards and Technology Special Publications

REF002	NIST SP 800-14	“Generally Accepted Principles and Practices for Securing Information Technology Systems”
REF003	NIST SP 800-16	“Information Technology Security Training Requirements, a Role and Performance Based Model”
REF004	NIST SP 800-18	“Guide for Developing Security Plans for Information Technology Systems”
REF005	NIST SP 800-26	“Security Self-Assessment Guide for Information Technology Systems”
REF006	NIST SP 800-30	“Risk Management Guide for Information Technology Systems”
REF007	NIST SP 800-33	“Underlying Technical Models for Information Technology Security”

REF008	NIST SP800-55	“Security Metrics Guide for Information Technology (IT) Systems”
REF009	Issues Related to Electronic Transmission of Data by Substance Abuse Providers in Illinois	
REF010	Websites Resources	

SECTION 7 Key Word Index

SECTION 8 Popovits & Robinson Attorney Contributors