

Final HIPAA Security Rule

William R. Braithwaite, MD, PhD

18 February 2003



HIPAA Security Rule Standards

9 Administrative Safeguard Standards

- 12 Required Implementation Specifications
- 11 Addressable Implementation Specifications

4 Physical Safeguard Standards

- 4 Required Implementation Specifications
- 6 Addressable Implementation Specifications

5 Technical Safeguard Standards

- 4 Required Implementation Specifications
- 5 Addressable Implementation Specifications

9 Administrative Safeguard Standards

Security Management Process

Assigned Security Responsibility

Workforce Security

Information Access Management

Security Awareness and Training

Security Incident Procedures

Contingency Plan

Evaluation

Business Associate Contracts and Other Arrangements

12 Required Administrative Specifications

Risk Analysis

Risk Management

Sanction Policy

Information System
Activity Review

Assigned Security
Responsibility

Isolating Health care
Clearinghouse Function

Security Incident
Response and Reporting

Data Backup Plan

Disaster Recovery Plan

Emergency Mode
Operation Plan

Period Evaluation of
Security Policies and
Procedures

Written Business
Associate Contract or
Other Arrangements

11 Addressable Administrative Imp Specs

Workforce Authorization
and/or Supervision

Workforce Clearance
Procedure

Workforce Termination
Procedures

Access Authorization
Management

Access Establishment
and Modification

Security Reminders

Protection from Malicious
Software

Log-in Monitoring

Password Management

Contingency Plan Testing
and Revision Procedure

Applications and Data
Criticality Analysis

4 Physical Safeguard Standards

Facility Access Controls

Workstation Use

Workstation Security

Device and Media Controls

4 Required Physical Imp Specs

Workstation Use

Workstation Security

Media Disposal

Media Re-use

6 Addressable Physical Imp Specs

Facility Contingency Operations

Facility Security Plan

Facility Access Control and Validation
Procedures

Facility Maintenance Records

Media Accountability

Data Backup and Storage

5 Technical Safeguard Standards

Access Control

Audit Controls

Integrity

Person or Entity Authentication

Transmission Security

4 Required Technical Imp Specs

Unique User Identification

Emergency Access Procedure

Audit Controls

Person or Entity Authentication

5 Addressable Technical Imp Specs

Automatic Access Logoff

Access Encryption and Decryption

Mechanism to Authenticate Electronic Protected Health Information

Transmission Integrity Controls

Transmission Encryption