

# SECURITY RULE COMPLIANCE SUMMARY CHECKLIST

## ADMINISTRATIVE SAFEGUARDS

STANDARDS	IMPLEMENTATION SPECIFICATIONS  (R) is required; (A) is addressable	STATUS		
		Done and Documented	N/A and Documented (may not apply if "required")	In Progress
Security Management Process	Risk Analysis (R)		-----	
	Risk Management (R)		-----	
	Sanction Policy (R)		-----	
	Information System Activity Review (R)		-----	
Assigned Responsibility	(R)		-----	
Workforce Security	Authorization and/or Supervision (A)			
	Workforce Clearance Procedure (A)			
	Termination Procedures (A)			
Information Access Management	Isolating Clearinghouse Function (R)			
	Access Authorization (A)			
	Access Establishment and Modification (A)			
Security Awareness and Training	Security Reminders (A)			
	Protection from Malicious Software (A)			
	Log-in Monitoring (A)			
	Password Management (A)			
Security Incident Procedures	Response and Reporting (R)		-----	
Contingency Plan	Data Backup Plan (R)		-----	
	Disaster Recovery Plan (R)		-----	
	Emergency Mode Operation Plan (R)		-----	
	Testing and Revision Procedure (A)			
	Applications and Data Criticality Analysis (A)			
Evaluation	(R)		-----	
Business Associate Contract	Written Contract (R)			

*(continued on next page)*

Copyright 2005 by Professional Risk Management Services, Inc. (PRMS, Inc.)

This publication is intended solely to provide general information on risk management issues. It is not intended to constitute legal counsel and should not be relied on as a source of legal advice. If legal advice is desired or needed, a licensed attorney should be consulted.

## PHYSICAL SAFEGUARDS

STANDARDS	IMPLEMENTATION SPECIFICATIONS  (R) is required; (A) is addressable	STATUS		
		Done and Documented	N/A and Documented (may not apply if "required")	In Progress
Facility Access Controls	Contingency Operations (A)			
	Facility Security Plan (A)			
	Access Control and Validation Procedures (A)			
	Maintenance Records (A)			
Workstation Use	(R)		-----	
Workstation Security	(R)		-----	
Device and Media Controls	Disposal (R)		-----	
	Media Re-use (R)		-----	
	Accountability (A)			
	Data Backup and Storage (A)			

## TECHNICAL SAFEGUARDS

STANDARDS	IMPLEMENTATION SPECIFICATIONS  (R) is required; (A) is addressable	STATUS		
		Done and Documented	N/A and Documented (may not apply if "required")	In Progress
Access Control	Unique User Identification (R)		-----	
	Emergency Access Procedure (R)		-----	
	Automatic Logoff (A)			
	Encryption and Decryption (A)			
Audit Controls	(R)		-----	
Integrity	Mechanism to Authenticate Electronic PHI (A)			
Person / Entity Authentication	(R)		-----	
Transmission Security	Integrity Controls (A)			
	Encryption (A)			

**REMEMBER:** The Security Rule is **scalable**, so you have the flexibility to implement security measures that are appropriate for your practice. HHS has indicated that the following factors can be considered in determining which measures to implement:

- \* the size, complexity, and capabilities of your practice
- \* your technical infrastructure, hardware and software capabilities,
- \* the costs of the security measures, and
- \* the probability and degree of potential harm from potential risks to electronic protected health information.

Also, you may already have many of these security measures in place to protect your patients' confidential, electronic information. It may be that you simply need to document existing security policies and procedures and document why other addressable security measures, if not implemented, are not needed.