

**HIPAA SECURITY RULE STANDARDS  
WORK PLAN**

Revised: - 1/10/08

Standards	Citations	Implementation Specifications R = Required, A = Addressable	Assigned Team	Implementation Solution	Status
<b>Administrative Safeguards</b>					
Security Management Process	164.308(a)(1)	Risk Analysis – R Risk Management – R Sanction Policy – R Information System Activity Review – R (Audit)	Multiple Multiple HR ST	NCHICA Tool – Review Stages NCHICA Tool – Review Stages HR Policy <sup>1</sup> SE-9: Auditing Information System Access	Completed Completed Completed Completed
Assigned Security Responsibility	164.308(a)(2)	- R	MHC	Responsibility Assigned to ND (Security Officer)/JB (Technical Advisor). Memorandum dated 12/4/03/Memo Regarding Local SO – 2/19/04	Completed
Workforce Security	164.308(a)(3)	Authorization and/or Supervision – A Workforce Clearance Procedure - A Termination Procedures – A	Multiple CI/HR ST/HR	SE-1: Authentication/Access Policy CI-001 Background Checks Policy SE-1: Authentication/Access Policy –Termination Checklist	Completed Completed Completed
Information and Access Management	164.308(a)(4)	Isolating Health Care Clearing House Function – R Access Authorization – A Access Establishment and Modification - A	MHC ST, PV ST, PV	Not Applicable SE-1: Authentication/Access Policy PV-10: Minimum Necessary Policy	N/A Completed Completed
Security Awareness and Training	164.308(a)(5)	Security Reminders – A  Protection from Malicious Software – A Log-In Monitoring – A Password Management – A	ST  NST, NIT NST, NIT NST	PV-16: HIPAA TEA/HCPRO Application/ Newsletter Articles, Etc. SE-5: Workstation Use & Security PV-10: Minimum Necessary Policy SE-1: Authentication/Access Policy	Ongoing  Completed Completed Completed
Security Incident Procedures	164.308(a)(6)	Response and Reporting – R	NST, ST	SE-6: Security Incident Response	Completed
Contingency Plan	164.308(a)(7)	Data Backup Plan – R Disaster Recovery Plan – R Emergency Mode Operation Plan – R Testing and Revision Procedure – A Applications and Data Criticality Analysis - A	Multiple Multiple Multiple Multiple Multiple	IS Disaster Recovery Plan Template IS Disaster Recovery Plan Template IS Disaster Recovery Plan Template IS Disaster Recovery Plan Template IS Disaster Recovery Plan Template	Approved/ Pending Implementation
Evaluation	164.308(a)(8)	- R	Multiple	Ongoing Organizational Effort	CHAN/DT/Etc.
Business Associate	164.308(b)(a)	Written Contract or Other Arrangement - R	NIT, PV, CSG	Security Rule requirements addressed in revised MHC Business Associate Agreement/Addendum	Documents Complete: 01/04

<sup>1</sup> Healthcare organizations that have in place HR policies for “corrective or disciplinary action” that assign sanctions or actions will meet this Security standard.

Standards	Citations	Implementation Specifications R = Required, A = Addressable	Assigned Team	Implementation Solution	Status
Contracts & Other Arrangements				templates (January, 2004). Communicated to MHC P Team/PM/JB/SP/ BD	Identifying/Ongoing
<b>Physical Safeguards</b>					
Facility Access Controls	164.310(a)(1)	Contingency Operations – A Facility Security Plan – A Access Control and Validation Procedures – A Maintenance Records - A	FAC FAC FAC FAC	Facility Access/EOC Plan (JCAHO) Facility Access/EOC Plan (JCAHO) SE-1: Authentication/Access Policy Facility/Equip. Maintenance/EOC-JCAHO	N/A to IS N/A to IS Completed N/A to IS
Workstation Use	164.310(b)	- R	Multiple	SE-5: Workstation Use & Security	Completed
Workstation Security	164.310(c)	- R	Multiple	SE-5: Workstation Use & Security	Completed
Device and Media Controls	164.310(d)(1)	Disposal – R Media Re-Use – R Accountability – A Data Back-Up and Storage - A	Multiple Multiple NST, DT NST, DT	PV-6: Destruction/Disp/ReUse Policy PV-6: Destruction/Disp/ReUse Policy PV-6 & Local Inventory Controls Assigned to Disaster Recovery Team	Completed Completed Completed Drafted to CSG
<b>Technical Safeguards</b>					
Access Control	164.312(a)(1)	Unique User identification – R Emergency Access Procedure – R Automatic Logoff – A Encryption and Decryption – A	NST NST NST	SE-1: Authentication/Access Policy SE-1: Authentication/Access Policy SE-1: Authentication/Access Policy SE-3: E-mail Policy	Completed Completed Completed Completed
Audit Controls	164.312(b)	- R	NST	SE-9: Auditing Information System Access	Completed
Integrity	164.312(c)(1)	Mechanism to Authenticate PHI - A	Multiple	Covered in Multiple Privacy/Security Policies	Ongoing
Person or Entity Authentication	164.312(d)	- R	NST	SE-1: Authentication/Access Policy	Completed
Transmission Security	164.312(e)(1)	Integrity Controls – A Encryption - A	NST	SE-3: E-mail Policy	Completed

<b>Security Policies &amp; Documents</b>			
SE-1	Authentication Standards	SE-9	Auditing of Access to Protected Health Information
SE-2	Healthline Systems Credentialing Software-Tech Security	SE-10	Retention of E-Mail Transmissions
SE-3	E-Mail and the Use of Protected Health Information	SE-11	Portable Devices – Use & Security
SE-4	Remote Access – Tech Security Practices & Procedures	SE-12	Non-IT System Administrator Role, Access Controls, Etc.
SE-5	Workstation Use and Security	SE-13	Data Center Security
PV-6	Disposal/Destruction/Reuse of PHI	SE-14	IT System Administrator Role, Access Controls, Etc.
SE-6	Security Incident Response (Disaster Recovery)	SE-15	System Change Management
SE-7	IS Infrastructure – System Standards	SE-9	Auditing of Access to Protected Health Information
SE-8	Data Back-Up (Disaster Recovery)		