Technical and Non-Technical Evaluation

Security Walk-Through Checklist

Evaluation #:	Evaluation Date:	Performed By:

Workforce Member Conduct	Yes	No	Comments
Workforce members and visitors are wearing ID badges.			
Workforce members challenge people who are not wearing ID badges.			
Workforce members protect security of ePHI by speaking softly and, when appropriate, using nonpublic areas.			
Workforce members can identify the designated Security Officer and how to communicate with him/her.			
Workforce members understand security incident reporting procedures.			
Workforce members can identify disciplinary action that can be taken.			
Workforce members can identify violations that may result in disciplinary action.			
Workforce members understand their role in an emergency and to whom they report.			
Workforce members turn in removeable media (e.g. CDs and flash drives) to the Security Officer for identification.			
Workforce members only use or re-use removeable media when authorized.			
Workforce members with remote access understand acceptable behavior when accessing ePHI.			

Workstation Use	Yes	No	Comments
Workforce members protect user ID and passwords and do not share them.			
User ID's and passwords are not posted on or near workstations.			
Workforce members do not share workstations while logged in.			
Password change policy is enforced and passwords must be reset after ## amount of days.			
Workstation and Server Windows updates are current and installed regularly.			
Software install restriction is enabled and enforced for non-admin users.			
Workstations and computer monitors are positioned to prevent unauthorized persons from viewing ePHI or privacy filters are used.			
Documents with PHI are concealed or stored face down, specifically in public areas and when workforce members leave their workstations.			

Documents with PHI are stored or filed when not in use to avoid observation or access by unauthorized persons.			
Computers are locked and returned to the login screen either automatically or by the user and password authentication is required to access the workstation.			
EHR "park" or logoff is enabled and begins after ## minutes of inactivity.			
All computers are locked or shut down after working hours.			
Laptops or portable media equipment are physically secured.			
PHI on printers, copiers, or fax machines is always attended by staff.			
Backups of ePHI are secured in a safe area (e.g. offsite or in a fireproof safe).			
PHI is shredded or discarded in a secure container.			
Anti-virus/Anti-malware is installed on all workstations and servers.			
Anti-virus/Anti-malware definitions are current on all workstations and servers.			
Access Controls	**Yes**	**No**	**Comments**
Workforce vetting procedures are documented.			
Approval for user access to ePHI systems is documented and updated when permissions are modified.			
All workforce members have unique user IDs for the network and ePHI systems.			
Doors with access-control mechanisms, such as locks or key cards, are closed and not propped open.			
Access to computer room is restricted to authorized personnel.			
Access to fax machines and printers is limited to authorized staff.			
Accerss to the wireless network is only available to authorized workforce members.			
Office doors, filing cabinets and desks are closed and, if they contain PHI, locked when unoccupied or unused.			
After hours, office doors, filing cabinets and desks are locked.			
After hours, building alarm is properly armed.			
Workforce members with keys, access codes, alarm codes and/or key cards are documented.			
Server and/or network equipment is properly secured with a lock and not in a publicly accessible area (e.g. next to waiting room or connected a patient care hallway).			
Telephone closets/racks are locked so unauthorized persons cannot gain access to telephone lines.			

Environmental Controls	Yes	No	Comments
Fire escape plans are posted in public areas and easily visible.			
Smoke detectors and fire extinguishers are accessible and operational.			
Network / Server closet or room is properly cooled.			
Servers and network equipment are plugged into uninterruptible power supplies.			
Computer equipment is plugged into surge protectors and, where appropriate, uninterruptible power supplies.			
Data Access and Transmission	**Yes**	**No**	**Comments**
Wireless networks are encrypted to WPA-# standards.			
Mobile devices with access to ePHI are encrypted.			
Remote access controls are technologically enforced for all workforce members with remote access.			
Document Retention (6 years from the date it was last effective)	**Yes**	**No**	**Comments**
Security awareness training materials, security reminders, staff meeting minutes and other documentation is maintained.			
Current, fully executed Business Associates Agreements are on file with all business associates.			
Records/Log of maintance that may impact the security of the building (e.g. changing locks or access codes) is documented.			

Technical and Non-Technical Evaluation

Security Walk-Through Log

Evaluation Log

Purpose: To document planned and/or completed evaluations and summarize the results

Evaluation #	Evaluation Date	Evaluated By	Status	Improvement Opportunities	Comments	Referred to Risk Management
Evaluation # 1						
Evaluation #2						
Evaluation # 3						
Evaluation # 4						
Evaluation # 5						
Evaluation # 6						
Evaluation # 7						
Evaluation # 8						
Evaluation # 9						
Evaluation # 10						
Evaluation # 11						
Evaluation # 12						
Evaluation # 13						
Evaluation # 14						
Evaluation # 15						
Evaluation # 16						
Evaluation # 17						
Evaluation # 18						
Evaluation # 19						