

VITL Network and Practice Security Checklist



NETWORK MANAGER'S RESPONSIBILITIES

| Network Security | Date | Initials |
|---|------|----------|
| Conduct an external security scan to determine if there are any vulnerabilities via the Internet | | |
| Ensure the use of encryption during file transfer, both internally and externally | | |
| Ensure the health and status of the firewall and its configuration | | |
| Apply current firmware updates to any network device | | |
| Ensure the method and encryption for Remote Access for the practice - if used. NOTE: Use of direct RDP to internal network (directly through a firewall) is a known security risk and is not acceptable | | |
| Ensure that the wireless system's access is restricted to practice-owned devices, and connection is restricted and encrypted | | |
| Servers (if used) | | |
| Ensure that security patches and Operating System versions are up to date and a method for keeping them up to date is utilized | | |
| Ensure that Active Directory controls (or comparable controls) are in place for user privileges, as well as group policy best practices | | |
| Ensure that Backup Procedures are in place, including: <ul style="list-style-type: none"> • A policy for media protection, labeling, storage, transport, and encryption • An audit trail is kept of each night's backup | | |

| | | |
|--|--|--|
| Workstations and Laptops | | |
| Ensure that all PCs are at the current patch level for software security updates and a method for keeping them up to date is utilized | | |
| Ensure that Anti-Virus protection is in use on all devices and a method for keeping them up to date is utilized | | |
| Ensure that Anti-Spyware protection is in use on all devices and a method for keeping them up to date is utilized | | |
| Ensure that Anti-Malware protection is in use and a method for keeping them up to date is utilized | | |
| Ensure that laptops have encrypted hard drives for any device containing Personal Health Information | | |
| Documentation/Policies | | |
| Provide a network diagram showing server and workstation locations | | |
| Provide proof of regular auditing of the health of the network (Provide sample report) | | |
| | | |
| PRACTICE RESPONSIBILITIES | | |
| Ensure the server is in a secure location | | |
| Ensure that a Disaster Recovery plan is defined, including: <ul style="list-style-type: none"> • System Recovery method • Data Restoration method • Data access when practice site is not available | | |
| Ensure there is a policy for copying data to portable and mobile devices, such as flash drives or iPods | | |
| Ensure there are policies and procedures to prevent theft of workstations, servers, laptops | | |
| Ensure that a Log-in and Password policy have been established | | |

| | | |
|---|--|--|
| Provide an access diagram or list (who has access to what) | | |
| Ensure that device passwords are documented and kept in a secure location | | |
| Ensure that the practice has a policy for email encryption when sending Personal Health Information | | |
| Ensure that a HIPAA Business Associate agreement is in place with partners | | |
| Name and Signature of both Network Manager and Practice Manager | | |
| Date | | |