CURRAN DATA TECHNOLOGIES

Guiding You Through Your Cybersecurity and HIPAA Compliance needs.

13 tips from the FBI to thwart healthcare hackers

1. **Highlight awareness of threats –** Enhance employee awareness about malware threats and train appropriate individuals on information security principles and techniques
2. **Update patches on operating systems** – Patch the operating system, software and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This precaution can be made easier through a centralized patch management system.
3. **Automatically update anti-virus and anti-malware** – Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
4. **Limit use of privileged accounts** – Manage the use of privileged accounts by implementing the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary; they should operate with standard user accounts at all other times.
5. **Reduce the extent of privileges –** Configure access controls with least privilege in mind. If a user only needs to read specific files, he/she should not have write access to those files, directories or shares.
6. **Beware of macro scripts** – Disable macro scripts from office files transmitted via e-mail.
7. **Restrict software use** – Implement software restriction policies or other controls to prevent the execution of programs in common malware locations.
8. **Institute regular backups** – Regularly back up data and verify the integrity of those backups.
9. **Ensure backups are secure and separate** – Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing them offline.
10. **Use application 'whitelisting'** – Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
11. **Make use of virtualized environments –** Use virtualized environments to execute operating systems or specific programs.
12. **Categorize and protect sensitive data** – Categorize data based on organizational value and implement physical/logical separation of networks and data for different organization units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization's e-mail environment.
13. **Require user interaction for key applications** – Require user interaction for end user applications communicating with Web sites uncategorized by the network proxy or firewall. Examples include requiring users to type information or enter a password when their system communicates with an uncategorized Web site.