HIPAA SECURITY SUITE
Your key to HIPAA compliance®

Tel: 949.474.7774 • 800.970.0402 • fax: 949.474.7775
Web: acentec.com • Email: info@acentec.com
Offices Located Nationwide

12 Most Common Medical Practice Technology Security Mistakes

1. Sharing of usernames and passwords —often done out of convenience, the personal liability employees now face should motivate employees to change this behavior.
2. Not logging out before leaving a workstation — again, primarily a matter of convenience, this creates a serious concern. An unattended workstation with access to PHI is a clear HIPAA violation.
3. Passwords are too easy — in most cases this can be prevented in the EHR as well as in the operating system, but if enhanced password settings aren't being used, most users revert to overly basic passwords that are easily hacked. Your employees should be encouraged to use passwords that, at the very least, include capital letters and numbers.
4. Mobile devices that lack security — lack of encryption and ability to remotely wipe, for example.
5. Faxing to incorrect or unattended fax machines — numerous HIPAA fines have been levied due to fax related breaches.
6. Using e-mail communication that is
    a. unencrypted
    b. Web-based
7. Inadequate or improperly configured firewalls — in most cases, firewalls designed for home use do not meet the security and configuration requirements HIPAA calls for. Simply having a firewall doesn't guarantee it's configured securely. Managing traffic appropriately at the firewall level is essential to keeping your electronic patient records safe.
8. Lack of intrusion prevention — unlike most firewalls, intrusion prevention devices (or software) use regularly updated intrusion definition databases to assist them in keeping your network locked down from the outside world.
9. No antivirus, or expired antivirus — keeping your antivirus definitions database up to date is as important as having it in the first place. The easiest way to manage the antivirus software in your practice is to use a centrally managed solution. Popular programs like AVG include network manageable antivirus software.
10. Weak, or no wireless encryption — in most cases, gaining wireless access to your network is the equivalent of giving a hacker a seat in front of your server. Although any encryption is better than nothing, if you are not using the Advanced Encryption Standard (AES), you may not meet HIPAA standards for PHI.
11. Patches not being installed — Microsoft issues software updates on the second Tuesday of each month (known as "Patch Tuesday"). Critical updates may be released anytime. Many of these updates are security related. Not keeping your server and your workstations up to date unnecessarily exposes your entire network.
12. Use of Windows 10 personal in a healthcare setting — Windows 10 personal lacks the encryption and security features of the business grade Windows alternatives. It's better than an outdated version of Windows, but it should be on your short list of upgrades.