

Cybersecurity Tips

1. When traveling by plane or train, always keep your laptop with you and never check it with your luggage. When traveling by car, keep your laptop out of sight. Security experts also advise that you affix your contact information along with a promise of a reward on your laptop to improve your odds of getting the computer back in the event it goes missing.
2. Saying no to patients because of the practice's policies can be difficult. You can use the LAEA approach: Listen, Acknowledge, Explain, Apologize.

For example: Listen until they are done speaking and then say, "Mr. Patient, I know it seems like it would be simple for us to put your records on your USB drive. The reason we cannot do it is because we are committed to protecting PHI, including yours! I am truly sorry, and I will be happy to provide you with a copy of your health records within X business days."

3. When sending email *remember* to encrypt them. Some email applications allow you the option of sending encrypted or not encrypted. When in doubt, encrypt.
4. There are many sanitization tools and methods available online to help clear disk drives of sensitive data. A quick and easy way to narrow your search is to check out the NIST Federal Agency Security Practices website at http://csrc.nist.gov/groups/SMA/fasp/documents/production_io_controls/proc_media_sanitization4.doc to see what tools other federal agencies are using to sanitize disk drives.
5. Type in a temporary password while on the phone with tech support. Ask them to hold while you change your password. Copy the password *carefully* so that when the system asks for your "old" password, you can paste or type it in in order to make the change to your new password. Changing your password immediately prevents you from losing or forgetting the temporary one provided by tech support. Don't forget to either destroy the written password or secure it safely in a locked drawer or cabinet.
6. Rely on the HIPAA Privacy and Security Rules. When faced with someone who doesn't understand the importance of protecting PHI, simply explain to the individual that patient health records are protected by HIPAA, and all covered entities are required to secure patient health information.

7. Changing the screen saver settings on your tablet can increase security by having a sleep setting require a password and having it activate after a very short period of inactivity. Consult your tablet's manual.
8. Store passwords in a locked drawer, cabinet or other secure place. You can also save your passwords on a secure device or use a special software program especially designed to securely store ALL of your passwords. Follow the instructions on the software to ensure you use it correctly.
9. Create a checklist of the actions you need to take to ensure mobile devices are secure before issuing them to new or existing employees.
10. Developing effective risk management strategies is key to the success of any medical practice and can minimize the possibility of adverse events like loss of patient information through unsecured networks. HHS has a short, easy to use risk management guide that lists common risks and how to mitigate them. It's a useful benchmark document to keep in your office.
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remotese.pdf>
11. Make sure all providers and staff are familiar with the back up and recovery plan and understand their role in the plan.
12. Ensure that staff understand the practice's expectations for use of computers, mobile devices and software. This should be part of annual security/privacy staff training. Consider acquiring legitimate software that blocks potentially offensive, dangerous or questionable websites.
13. Passwords should be changed regularly, and users should be prevented from reusing at least their last 2-3 passwords. By requiring passwords to change quarterly you help prevent passwords from being discovered and used illicitly.
14. The destruction of PHI that is no longer required under the practice's retention policies is an important element of protecting patient information. Properly disposing of PHI should be part of a routine process and documented in the practice's policies.
15. Ensure user accounts for former employees are appropriately and timely disabled. If an employee is to be involuntarily terminated, access to the account should be disabled before the notice of termination is served.

16. Wireless routers should be appropriately encrypted. Encryption modes are specified in IEEE standard 802.11i. The correct encryption modes are WPA2 or WPA, *not* WEP.