Health Information Compliance Alert

Privacy: Keep Your Remote Workers' Information Private With This Sample Document

Make sure your offsite workers are aware of security and privacy concerns.

Your practice has tough decisions to make when allowing employees to handle patients' private health information (PHI) while working from offsite locations. You may require encryption, you may prohibit them from working on their personal laptops when dealing with PHI, or you may even only allow remote work when it's done for emergency reasons. But no matter what, you need to communicate your privacy expectations to your employees.

Consider this sample document as a guide, contributed by **Glenn Allen,** information security director with **Fairview Health Services** in Minneapolis, Minn.:

Security Considerations/Guidelines for the Remote Worker: When working remotely, we expose [organization name] to increased risk of privacy and security incidents and breaches. [Organization name] takes great care in protecting the privacy and security of its paper and electronic systems in order to safeguard its patient (and other confidential) data. Remote workers need to take the same care.

• Only use a currently supported operating system (e.g., XP or Vista) with all available security patches.

• Use auto-updating antivirus software. Antivirus with outdated virus definitions has reduced effectiveness.

• Use a properly configured firewall. Also strongly consider having a properly configured router between your equipment and internet connection (which can greatly increase your protection as well).

• Be careful when using shared (family) computer equipment to access [organization name] resources. The computer you share can inadvertently be compromised by others. It may make sense to limit access to equipmentused to connect to [organization name] unless you understand what others are using the computer for.

• Do not use any form of file sharing programs on equipment used to connect to [organization name] resources. Many file sharing programs can be used to open or share folders and files on your own computer (sometimes without the user meaning to).

• Get guidance from your operating system vendor on safe computing. Many OS vendors (like Microsoft) have great resources for both end-user and IT professionals.

• Never reply to, open links in or attempt to unsubscribe to unsolicited emails. Just following a link in an email to a hostile site can compromise your computer.

• Immediately report any security concerns to your manager or the IT department.

• It is required that comprehensive steps be taken to make sure that only programs directly related to the employee's business purpose are run while being connected to [organization name]'s network.

• Position your monitor so that unauthorized person/s cannot view the screen.

• User ID and/or passwords may not be shared or written, taped or stored on the computer/laptop, in the computer bag or in any location relative to the computer.

• Be careful when printing confidential documents. Be sure you are printing to the correct printer and that you are able

to retrieve any confidential documents quickly.

• Be aware when using wireless hotspots. Some wireless hotspots may be run by unscrupulous individuals who are looking to steal/misuse data and equipment connected to the hotspot.

• [Organization name] may inspect and monitor data and communications at any time. This includes monitoring network usage (including contents), and examining files on any system that has been connected to the network.

• Be mindful when selling or getting rid of computer equipment. Remember to scrub or properly dispose of drives (including flash/thumb) so others cannot access confidential data.