Is Dropbox Putting Your Medical Practice's Compliance Plan at Risk?

Since its release in 2008, Internet File Storage tool Dropbox has been a big hit with people who have to keep track of files on multiple computers. Users can download a free program that lets them upload files to "the cloud" (see: a server or servers connected to the Internet), and then can access the files on any other device: other PCs or Macs, any web browser, even a smartphone or tablet. The program puts a small, "dropbox" in the bottom corner of the user's screen and any file dragged into the icon is automatically uploaded. When the user looks at the dropbox on another device, the file is there waiting.

Dropbox has been wildly popular because it is extremely useful: it saves people time and makes them more productive, and is free for the first 2GB of storage. Users can either earn more free storage by referring friends to the program, or purchase more storage with plans that start at $9.99 per month. There are also group plans that allow for centralized file sharing.

In fact, some of your employees could be using Dropbox in your practice right now to let them work from home or the road, or sync multiple work computers, or even give them access to work data on their mobile devices. As all healthcare management professionals know, this has the potential to be a huge problem. The data that is handled in many daily tasks in a medical practice is protected not only by patient confidentiality, but also by federal regulations with some serious financial teeth. On Dropbox's website, they go after the question head on:

> *"Unfortunately, Dropbox does not currently have HIPAA, FERPA, SAS 70, ISO 9001, ISO 27001, or PCI certifications. We'll update this page with any new certifications as we receive them, so please do check back"*

Dropbox is very useful for students, people on the go, and anyone who works from different places and different computers, but it's not really designed for auditable, granular protection of sensitive data. This isn't to say Dropbox isn't safe or secure – although they've had a few problems, they've taken steps to ensure they aren't repeated – they just aren't designed for the security needs of healthcare organizations. Even a great password policy in place for your group won't help if you are relying on tools that were not built for the industry.

So what can a practice do if it needs a cloud-based file hosting solution that can help your team work in different places without jeopardizing your compliance? At Manage My Practice, we use and endorse Box, a leading provider of enterprise class file storage. We like Box so much for healthcare purposes that we partnered with them to bring you FileConnect. Using the power of Box, which has installations in over 80% of the Fortune 500 companies, FileConnect supplies fully auditable, granular file storage to your practice while working in lockstep with your existing HIPAA compliance plan.

Click below to contact us to learn more about what FileConnect can do for you!

Click Here to Talk to Us About Fileconnect in Your Practice!