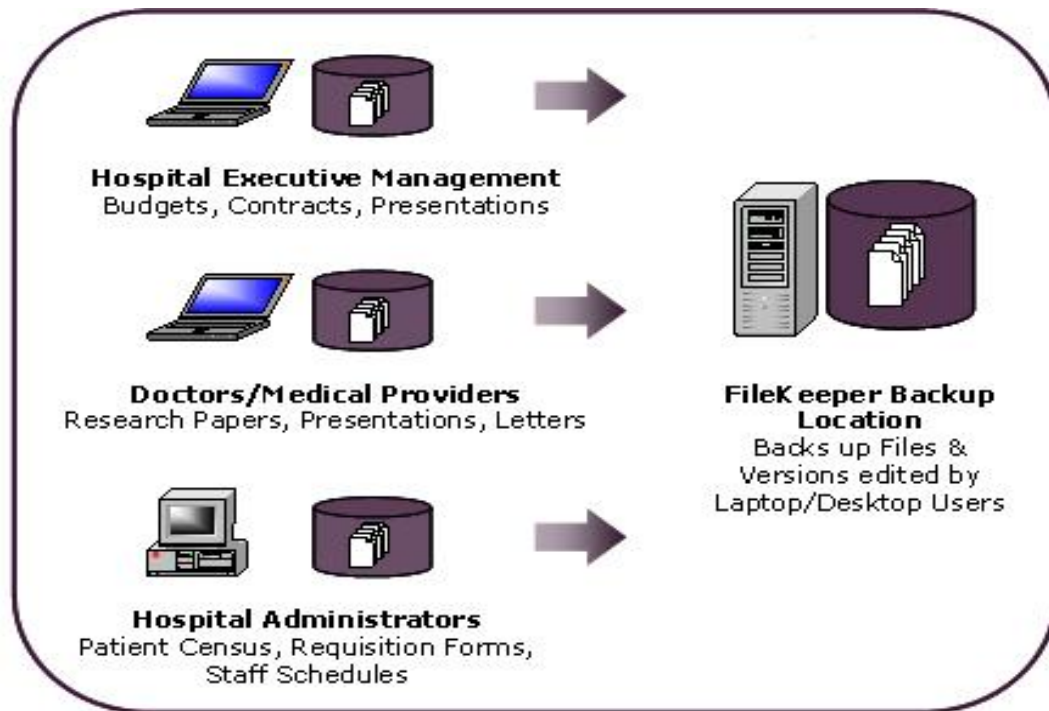


Yosemite FileKeeper Protecting Healthcare Data

Supporting healthcare has always been a challenge for IT. Adding to the challenge, healthcare organizations must now deal with an explosion in the number of mobile users, maintain compliance with HIPAA regulations and reductions in IT budgets and staff.

Yosemite FileKeeper provides healthcare organizations with a way to transparently protect data files such as Microsoft Word documents and Microsoft Excel spreadsheets created by physicians, nurses and hospital staff. FileKeeper provides real-time data protection of healthcare data whether healthcare Staff is connected to or disconnected from the facilities network.



What happens when your hard disk "flat lines?"

Most healthcare organizations employ a policy for staff to store data files on a network file server - yet very few organizations comply with this policy. In fact, a recent poll of 2,299 adults, conducted by Harris Interactive®, finds that more than a third (35 percent) of U.S. adults who have personal/professional data and digital information stored on a PC or a laptop never back up their files, and a vast majority (76 percent) of those who do back up their files don't do it often enough.

The fact is that healthcare professionals store files where it is most convenient, which often includes the local hard disks of their laptop and desktop computers. Mobile users generally store files on the local hard drives of the laptop computers so

they can access the files while disconnected from the network.

So what happens to these files when the disk fails, is stolen or corrupted by virus activity?

Healthcare organizations turn to FileKeeper to ensure that data files stored on the local hard drives of their Windows laptop and desktop PCs are backed up to a secure file server. FileKeeper protects every file that every user modifies, regardless of whether the file is stored on the local hard drive of the user's PC, a network server or even a USB connected "thumb drive." FileKeeper gives healthcare IT managers' peace of mind knowing users can always restore any previous versions of their files when catastrophe strikes. When it comes to protecting healthcare data, a pound of prevention really is worth a pound of cure.

You just lost a laptop ... was it a HIPAA violation?

Yosemite FileKeeper provides healthcare organizations with the information they need to determine whether patient data is being stored on the local hard drives of their laptop and desktop computers.

Agent Activity Report		
User	brhymes	
Machine	FKLAB-WXP-LT01	
Backup location	All	
Date range	8/26/2005 4:23:41 PM - 8/27/2005 4:23:41 PM	

Date - the date and time of the operation
Operation - the operation that was performed, e.g., copying a new version to the backup location
Source File - the path to the source file
Destination File - the path to the destination file
Result - whether the operation succeeded or failed

Date	Operation	Source File
8/27/2005 3:46:11 PM	Version	C:\Documents and Settings\brhymes\My Documents\Marketing\Mailing List\Mailing List (4-4-05).xls
8/27/2005 3:45:59 PM	Version	C:\Documents and Settings\brhymes\My Documents\Marketing\Mailing List\Mailing List (4-4-05).xls

In the event of a lost or stolen laptop, FileKeeper can help determine whether patient data was compromised by providing a complete catalog of the data files that were stored on the laptop at the time it was lost/stolen. FileKeeper also provides HIPAA compliance auditors with access to a backup copy of files that were stored on the lost/stolen laptop, providing them with the ability to examine the contents of the stolen files.

As the old saying goes, you can't manage what you don't measure. FileKeeper provides healthcare organizations with the information they need to measure whether the information stored on their laptop and desktop computers is in compliance with their HIPAA policy.