



TECHNOLOGY

Medical Information Technology

Your Monthly IT Guide since 1995!

Electronic Health Records Can Get Sick Too: What Do You Need To Know To Prevent a Crisis?

Bernd Wollschlaeger, M.D., FFAFP, FASAM

Information Technology tools are an integral part of modern health care delivery. Whereas a decade ago physicians using computers in their medical practice were considered geeks, today's medical students, interns and residents cannot imagine practicing medicine without it. The integration of electronic health records into the practice of medicine created new challenges and problems that we need to consider. The most important reality we have to accept is that each tool requires care and maintenance. Imagine driving your car everyday ignoring the warning light that an oil change is overdue. Eventually, the engine will stall and you face two equally costly choices: buy a new car or a new engine.

Computers may not require lubrication but they can stall too unless you pay attention to a regular maintenance schedule. Often, warning lights will not appear before a computer crash occurs. Can you imagine that your entire system crashes in the middle of a busy day with a waiting room full of patients? If you should hear the whining sound of a dying hard disk you better make sure to have backed up your data.

So what can you do to prevent an inevitable crisis?

First, you have to identify four essential components of your information technology system: hardware, software, network and data integrity & security. Create an inventory of each and every component including when it was last upgraded, replaced, or maintained. Then identify IT personnel for a quarterly or six-month checkup of each component. Contracted vendors can offer on-call support or remote monitoring. For larger practices with more complex systems dedicated health IT staff may be required for whom the checkups are part of a job description.

Second, you should know where your precious patient and billing data is being stored. Is it hosted on a remote server or does the data reside on a local server (or servers) within your practice? If your patient data resides inside the practice then you need to test them regularly for potential failures. Check the main server (s) to ensure that everything is running properly, but backup systems MUST be checked as well.

Make sure that backups are running properly. Instruct your staff to conduct regular data recovery drills pretending that the servers crashed and all data was lost and perform a practice run of restoring data from their backups. Sounds scary but imagine you learn that your ONE and

ONLY backup does not work!! Many small practices use web-hosted systems, also called Application Service Providers (ASPs), in which software vendors guarantee the maintenance of your patient data, which resides remotely on the vendor's server. In those circumstances you have to make sure that the vendor contractually is obligated to guarantee the integrity and safety of your data. Furthermore, you need to make sure to monitor the workstations inside the practice, especially secure them from unauthorized third-party access.

Third, you must make sure that your network is secured and meets federal requirements or standards. These include HIPAA regulations that need to be in place, such as audit controls. For medical practices I almost always prefer a hardwired network to a wireless network to ensure data integrity and privacy. You always have to stay up-to-date with your firewall and anti-virus software and you must test their functionality regularly.

How can you ever meet all of the above requirements?

Very simple. All of you can obtain more information and access technical support by enrolling in the South Florida Regional Extension Center. You can sign-up online at <http://www.southfloridarec.org/> <<http://www.southfloridarec.org/>

Don't wait! Start transforming your practice today!

I look forward to reading your comments and suggestions on our blog at <http://miamimedblog.blogspot.com/> or send me a tweet at <http://twitter.com/dadedoc>.

Disclosure: The author is a practicing family physician, addiction specialist and computer consultant. In addition, he is a founder and managing partner of a medical IT company and a member of the SFREC Steering Committee