

Interfaces: it is one of the most appealing features to EHR systems today, the ability to capture patient data from medical equipment immediately into the electronic chart. It eliminates the steps of manually recording the information and entering into the computer or scanning the paper results in and attaching the image to the chart. It also leads to some of the most frustrating moments of using an electronic charting: software support fingerpointing. This is an issue I deal with at least every week if not more, for example: the lab company {insert practice management system, ultrasound machine, or other medical equipment manufacturer} says their part of the interface is doing what it is supposed to and the EHR vendor says its software is working the way it is supposed to. Yet, the results are not coming from said equipment to the chart and neither company will provide any additional support as to why it is not working. Now what do you do? Let's take a closer look at what an interface consists of, why this fingerpointing occurs, and some ways to keep your interfaces active.

First, the interface itself; and for the most part software interfaces are the same today as they have been for years. Software A writes a file, in a certain format, to a specific directory every so many minutes. Software B looks at the directory every so many minutes to see if a new file exists. Sounds pretty simple doesn't it? The complicated part has to do with networks, permissions, clocks, programs running in the background, the starting and stopping of services, and even antivirus software. Computers are very precise, processing is either on or off, black or white, there is no in between so if every aspect is not exactly how the software is programmed to accept it, then it does not apply the file. Unfortunately, the real world doesn't operate that way, and we have power surges, our PC's are setup to automatically update the time via the Internet, a person loads new software on a machine or some other interrupting factor occurs.

The fingerpointing: adding to this dilemma are a slew of interfaces written and released quickly by companies (looking to cash in on a booming new market) which are not adequately tested. In early EMR days, we as resellers were told about interfaces to one practice management system or piece of equipment so we would go out and sell them, only to find out no one had ever implemented a particular interface. Just as frustrating would be the fact that when we called our vendor for technical support on an interface no one there knew how it worked either. This was mostly due to the fact that the EMR vendors did not write their own interfaces; they just resold them so they had no developers they could call on to describe how it was supposed to work and what was done to test it. Fortunately for us, our extensive computer experience and downright perseverance led us to become the people our vendor called to help their direct customers because we knew more about the interfaces they sold than they did. We had our own live customer installations and we also learned which interface companies to avoid no matter what they promised.

Some things to keep in mind when purchasing an EHR regarding interfaces: Ask to see a demonstration of what the results look like in the EHR. Also, ask who the interface is written by and who provides support for the interface, and get it in writing. See if you can call some references specifically to ask about the particular interfaces promised: ask the references how well they work, how easy are the results to interpret and move to a chart, what issues have they had with a particular interface, how were they resolved.

The quality of software system interfaces has improved over the last five years, however the inter company fingerpointing still exists to some extent. Since most of today's error end up being plain old human error, we recommend the following:

- 1) The physical computer where the interface software resides should not be used a regular workstation, it should be on a server, and a server should never be a workstation where someone sits and enters information all day.

- 
- 2) Do not allow unauthorized software or files to be downloaded to the machine that houses the interface, they could disable it or disrupt the path. Unauthorized software includes smiley faces, screen savers, and AOL Instant Messenger to name a few.
  - 3) Have more than good surge protection on any PC that runs any interface. Power blips may not be enough to shut down a machine, but can easily stop some of the processes that need to run continually like an interface