EMR and E-Discovery Part Two: On the Audit Trail

August 28, 2017
Health Care Alert

Attorneys

David H. Levitt

In part two of our series, EMR and E-Discovery, author David Levitt delves into audit trails, a type of metadata that creates a chronological record of access and changes to the data, and explains why an audit of metadata parameters could be a valuable risk management tool to healthcare institutions.

Recap of Part One:

- The intersection of Electronic Medical Records (EMR) and e-discovery is in the very early stages.
- Recognition of the risks affiliated with e-discovery of EMR can impact important aspects of how medicine is practiced and the establishment of healthcare institution policies.
- Most state court systems have only recently begun developing their own rules and will likely go through their own difficult learning curve, causing expense and angst for healthcare institutions.
- Questions arise over how the use of EMR affects the integrity of a patient's chart.

Within the last five years, articles by plaintiffs' attorneys who handle medical malpractice cases have discussed requesting "audit trails" in discovery. These are chronological records of access and changes to the data, and arguably a type of metadata. Notably, however, in some EMR systems, an option may exist to turn off the audit trail feature, suggesting that it may not always be captured automatically. That said, although beyond the scope of this post, there may be requirements not to exercise the option to turn off this feature—and wisdom may suggest that it is best not to use this option.

In general, metadata is created each time someone interacts with the software. Depending on the parameters set by the programmer, the metadata may capture the identity of the person accessing the program, the time of that access, the duration of that access, and actions occurring during that access.

Yet even here, there may be variations between software from different providers. In one recent case—not a medical malpractice case—an issue arose about when certain computer-aided drawings were created, and when each modification was made to each drawing. The software in that matter, however, only recorded the date that the record was originally created, and the date that it was *last* modified. It did not capture the interim occasions of access or work on the drawings. That was the nature of that particular software.

That may vary among EMR software providers, depending on the particular software at issue. Some may, like the CAD software described above, preserve only the last modification. Others may capture each occasion when the record was accessed or changed. Because this may vary between software vendors, determining the scope of metadata preservation inherent in the system, independent of any potential need for a "litigation hold" when such an occasion arises, gaining an understanding of each software's features can be a valuable risk management tool.

For example, a common issue in medical malpractice litigation is whether a physician did or did not review a certain notation in the patient's chart before taking or failing to take action. Before EMR, the issue was largely one of credibility. A doctor might testify regarding which records he or she reviewed, or a nurse might testify to his or her communications (in writing or orally) with the doctor. EMR, however, has the potential to change this equation, to the extent that it captures and retains each log-in to the system, if it shows who logged in, when the person logged in, which records were reviewed, the duration of the review, and any actions taken around that time, with time stamps. Or, the *absence* of a record might be argued to be evidence that the person did *not* look at the chart or a particular entry in the chart at the relevant time.

This is not to suggest that one EMR system is better than another or that less metadata is better than more (or the reverse), but merely to highlight the need for risk managers to be *aware* of what is or is not retained automatically in the system, and to manage that process accordingly. For example, it can be essential in a given case that the practitioner and his or her attorney review such metadata as may be available *before* the practitioner makes a statement or gives deposition testimony that may turn out to be at odds with what the EMR record shows.

Additionally, most healthcare institutions use multiple software programs from multiple vendors—so there is likely no one right answer for any one institution. Medical devices are also run by software, and may have their own set of electronic records and metadata entirely separate from that in the main EMR system. An audit of metadata parameters for each applicable system could be helpful in an overall EMR management program.

Most of the major EMR vendors have established systems by which they receive feedback from their customers in order to make their products better. But, having spoken with some vendors in the course of negotiations, this feedback rarely if ever includes commentary about the potential litigation or practice-changing aspects of EMR in the medico-legal context. Articles have been written about how EMR can itself create the possibility of medical liability claims different from those based on paper charts. We have not seen, however, publications discussing how the vendors might improve their offerings to make them more user-friendly for e-discovery.

Beyond merely providing feedback, medical institutions might consider whether they want to insist on changes to the software in the process of negotiating the license or an extension itself. The ability to manage such things as metadata and access may itself be a differentiator between different vendors that can impact the decision regarding which vendor's product to license.