HINSHAW

Alerts

EMR and E-Discovery Part Three: All Systems Go

September 5, 2017
Health Care Alert

In part three of our series, EMR and E-Discovery, author David Levitt details the current diagnostic tools utilized by modern health care as well as some of the considerations healthcare institutions should evaluate when making decisions about software and licensing.

Recap of Part Two:

- Audit trails are chronological records of access and changes to the data, and a type of metadata, which is created each time someone interacts with the software.
- Metadata can 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, but there may be variations between software from different providers.
- An audit of metadata parameters for each applicable system could be a valuable risk management tool and helpful in an overall EMR management program.
- Healthcare institutions might consider whether they want to insist on changes to the software in the process of negotiating the license or an extension on a license.

Modern health care involves the use of sophisticated diagnostic tools, from small hand-held devices to large machines that cost millions of dollars. Many of these devices are managed by software. Many require log-on IDs. And, like most software, they may capture metadata regarding who did what and when.

The metadata from the devices rarely makes it into a patient's chart. The end-result – a report, an image, the output from the device – will, but not the information in or about the machine itself. When was it last calibrated? What were the settings? A multitude of information about the device itself and the human interactions with the device can potentially be at issue in a given case. Yet how many healthcare institutions have steps in place to gather, preserve, and review that information on a regular basis, or when an incident occurs that might give rise to a claim? Most often, the parties will assume the accuracy of the reports from the device.

The volume of information available from the myriad of devices is almost certainly too much to preserve for more than a short period of time. For example, some in the trucking industry use sophisticated satellite tracking devices to monitor the location of trucks and progress in making deliveries. It is

Attorneys

David H. Levitt

©2025 Hinshaw & Culbertson LLP

impossible to maintain that much information on a regular basis – typically, a few days or less of such information is available in real time, and then overwritten or discarded. When an incident occurs, however, data for that vehicle and that driver for the short amount of time still available is frozen and preserved. Similarly, if it is impossible to collect and preserve device-related metadata on a day-to-day basis, institutions should evaluate the practicality of doing so once an incident arises suggesting that a particular device and its software might contain relevant information.

©2025 Hinshaw & Culbertson LLP

Even this may be impractical. Not every unfortunate medical result ends up in a claim – and often the institution has no reason to believe that a claim will arise merely because of a bad result, and no reason, therefore, to preserve evidence. Moreover, even where there is reason to believe that a claim might be made sufficient to trigger a general obligation to preserve evidence, it would be a rare occasion where it is immediately apparent that information from the device itself would be relevant, and therefore frozen and preserved. Nonetheless, as part of setting up an overall system to manage EMR risk, the ability to collect data from devices should also be evaluated.

Another consideration is that many EMR systems include dropdown menus that suggest – and sometimes mandate – selection of certain options to describe presenting symptoms or other features of information gleaned from the patient. On some occasions, none of the dropdown options may precisely fit the situation at hand, so selection of that option may present a less-than-accurate picture to the next practitioner (or even the same practitioner at a later visit).

While this potentially creates liability risks in itself, and therefore suggests that training on optimum use of the system can be an excellent method to mitigate the risk (accompanied by follow-up to confirm that practitioners exercise appropriate caution in selections and explanations in narrative boxes in the midst of busy days), dropdown menus present an additional concern because they are typically not included in the PDF print-out received by the attorneys. Or, even if the selected menu item is included, the other options available to the practitioner at the time of the entry may not be presented in the PDF version of the record.

Some EMR programs include a system of “alerts” that may pop-up on the screen while the provider is interacting with the EMR for a patient. Is the existence of the alert at a given moment recorded in the EMR, perhaps as metadata? Is the provider’s interaction with the alert recorded? Consider whether practitioners ought to be trained to provide some sort of feedback when an alert appears regarding whether it was followed or, if not, the reasons why not.

Here too, as attorneys become more familiar with the various features of different EMR programs over time, we should expect to see more plaintiffs’ counsel requesting more complete versions of the applicable EMR, in some reasonably useable electronic format, so that they can see the record as the practitioner saw it. Wisdom suggests, therefore, that healthcare institutions should be ahead of that learning curve, and develop strategies for responding to such requests as well as engaging in their own review as part of the development of defense strategy, both in any one particular case and as a matter of institutional policy.

©2025 Hinshaw & Culbertson LLP