Law Bulletin Publishing Company

January 2016 • Vol. 39 No. 1

Chicago Lawyer®

I’ve got a secret

Do-not-tell clauses in electronic record contracts real danger

Med-Mal Matters

Thomas A. Demetrio is a founding partner of Corboy & Demetrio, representing victims of medical malpractice and personal injury.

Kenneth T. Lumb is a medical-malpractice attorney and partner at Corboy & Demetrio.

In June, we discussed a study published in the *Journal of the American Informatics Association*, which concluded that many current electronic health record (EHR) programs display, aggregate or depict laboratory data and trends in ways that do not meet evidence-based criteria for laboratory data comprehension.

That study, titled “Graphical Display of Diagnostic Test Results in Electronic Health Records: A Comparison of 8 Systems,” evaluated the graphical displays of clinical laboratory results in eight EHRs using objective criteria for optimal graphs based on medical literature and expert opinion. The study concluded that none of the eight EHR programs met all of the performance criteria and that many of the programs contained flaws that could have a “significant, negative impact on patient safety.”

One thing the study did not reveal, however, was the identity of the potentially dangerous EHR programs. A recent Politico article reveals why that is.

One irony of this situation is that many of these systems are taxpayer-subsidized with $30 billion of stimulus funds from the Affordable Care Act.

The article, titled “Doctors barred from discussing safety glitches in U.S-funded software,” reports that some of the largest corporations selling EHRs insist that their customers sign contracts containing “gag clauses’” that prevent health-care providers from discussing problems with the software that could jeopardize patient safety.

In its research, Politico obtained through public records requests 11 contracts from hospitals and health systems in New York City, California and Florida that use six of the biggest vendors of EHRs. With only one exception, each of the contracts contained a clause prohibiting from public disclosure “large swaths of information.”

Politico reports that the clauses, included in contracts with Epic Systems, Cerner, Siemens, Allscripts, eClinicalWorks and Meditech, have prevented researchers from understanding the scope of the flaws in EHRs. For instance, Cerner’s contract with Los Angeles County’s health services department, worth up to $370 million, defines confidential information as “source code, prices, trade secrets, databases, designs and techniques, models, displays and manuals.” Such information, the contract states, can only be disclosed with the prior, written consent of the company.

The EHR companies argue that this language is necessary to protect intellectual property. But critics, like Elisabeth Belmont, corporate counsel for MaineHealth, contend that such language really acts to discourage health-care providers from reporting adverse events. According to Belmont, EHR vendors insists on confidentiality clauses because they don’t want to be ranked low by researchers or be tarnished by public reports of poor performance.

One particularly sensitive area, reports Politico, is sharing screenshots. Vendors often forbid their publication, citing the risk of giving their competitors an advantage in design or technology. Without screenshots, however, “it’s impossible to see the confusion that badly constructed software poses to a physician” or other health-care provider. A researcher at the University of Texas told Politico that he personally asked Epic’s CEO for permission to publish screenshots in a master’s thesis and was flatly rejected.

Which brings us back to the study in the *Journal of the American Informatics Association*. According to Politico, while the study disclosed which commercial systems it studied — Allscripts, Cerner, eClinicalWorks, Epic, Glassomics, Meditech, Partners HealthCare and the VA’s VistA system — it did not identify which graph belonged to which system.

The study’s authors obtained the screenshots from clinicians on the condition that the graphs would not be published with specific identifying information. According to the lead author, “T]he hospital employees fear for their jobs if they violate the policy of not sharing screens of the EHR.” Researchers have to beg for screenshots to study EHR performance but cannot disclose the identity of the underperformers.

One irony of this situation is that many of these systems are taxpayer-subsidized with $30 billion of stimulus funds from the Affordable Care Act. But the effect goes well beyond irony because flaws in commercial EHR systems pose a very real danger to patient safety.

Dr. John Sotos writes in his *Wall Street Journal* blog that EHRs are “killing and injuring people.” Sotos, a cardiologist and flight surgeon, argues that poorly designed EHRs “channelize” health-care providers’ attention away from the patient for even the simplest of charting tasks, the same kind of distraction that is a common human-factor contributor to airplane crashes.

According to Sotos, EHR vendors must recognize that the “human-computer” interface is more than just a way to look different than competitors. Rather, it is a critical component of a system that must be designed to be “undemanding of attention and cognition.”

Unfortunately, there’s not much chance of that happening as long as EHR flaws remain shrouded in secrecy. ■

TAD@corboydemetrio.com • KTL@corboydemetrio.com