FierceEMR

February 5, 2016

Health attorney Gerald DeLoss: Data sharing, use agreements in the midst of an evolution [Q&A]

By Marla Durben Hirsch

As data sharing continues to become more commonplace, the actions and use agreements that underpin these activities are transitioning to meet changing needs and concerns, according to health attorney Gerald "Jud" E. DeLoss, Esq.

DeLoss, a Chicago-based attorney with Clark Hill, is a nationally recognized expert in legal issues pertaining to health IT, software licensing, HIPAA and data exchange. He serves on the Illinois Health Information Exchange (ILHIE) advisory committee and the ILHIE data security and privacy committee.

Gerald "Jud" E. DeLoss Clark Hill Attorney

"[Such agreements] are being more specific about each party's obligations," DeLoss tells *FierceEMR*. "They're making sure that the person handling patient protected health information is using up-to-date technology, and adding to these contracts that their security officer can audit and review the other party regarding security of information."

In an exclusive interview, DeLoss shares his insights on developments in data sharing and use agreements.

FierceEMR: Now that more people are signing data use and sharing agreements, have the agreements themselves evolved?

DeLoss: They're becoming more complex. For instance, people are more skittish about data breaches [in light of the huge increase of them this past year].

People dealing with a business associate--such as a health information exchange--will no longer leave it to the business associate to ensure that it has policies on privacy and security. The data use and sharing agreements now spell out what the party demands from the business associate. In the good old days, people made representations that they had HIPAA policies even when they didn't [and covered entities didn't call them out on it]. Now covered entities are taking it more seriously.

It's also more common for the parties to be required to maintain cyberinsurance.

FierceEMR: Do people view the data itself differently from before?

DeLoss: There's an increased focus on de-identified data. There's a rush to make sure that de-identified information is not improperly used by other parties. They're also requiring any reporting of a security incident to include incidents involving de-identified information. There's a concern that it can be re-identified.

continued on pg 2

continued from pg 1

There's also a concern of the ownership and value of data, even though it's been de-identified. It has a financial benefit. It's a question of who controls it.

FierceEMR: Are there other ways that data sharing and use agreements are being reshaped?

DeLoss: I do a lot of work with behavioral health providers, and there's been an increased interest in the benefit and need to share all of a patient's medical records, not just physical health records. Some HIEs have been formed by behavioral health providers to exchange their information. They and payers are recognizing the need for holistic data compilation.

There also are more patients willing to put their behavioral health information in the HIE to give their providers a more complete picture so they can receive better care--catch drug-drug interactions, contraindications, etc.

While the current laws are very restrictive about sharing behavioral health data, there is legislative and regulatory activity to allow more of it. The House has introduced HR 2646 and the Senate has introduced SB 1945 to reduce the barriers to sharing alcohol and drug abuse patient records associated with 42 CFR Part 2, the regulation that governs the privacy of such records. The Department of Health and Human Services' Substance Abuse and Mental Health Services Administration released proposed rules Feb. 5, that would update the regulation and allow for more sharing of this data. These changes will affect the contracts.

FierceEMR: What are some of the challenges we're still facing?

DeLoss: Interoperability is still an issue, but people understand the need for it. The industry recognizes that voluntary steps, like Carequality, need to be taken.

There are also still different levels of concern among stakeholders regarding what goes on with the data being shared and how to protect it. There needs to be a common understanding and principles on that.

Gerald "Jud" E. DeLoss is a Member in Clark Hill's Chicago office in the Health Care Practice Group, Behavioral Health Care Practice Group, and Cybersecurity, Data Protection & Privacy Work Group. Jud represents a wide range of health care clients, including behavioral health care (substance use disorder and mental health) providers, health information technology (HIT) vendors, federally-qualified health centers (FQHC), hospitals, and research organizations. Jud also represents state and national health care trade and professional associations. He has extensive experience representing clients on compliance, privacy and data protection, reimbursement, fraud and abuse, and other health care regulatory and transactional matters. **Contact him at: gdeloss@clarkhill.com or (312) 985-5925.**