JUNE 02, 2017

THE MDLIVE CLASS ACTION: UNDERSTANDING THE COMPLEX RELATIONSHIP OF CONSUMER TELEHEALTH PLATFORMS

On April 18, 2017, a class action was initiated against MDLive, Inc. asserting that MDLive inappropriately collected and disclosed patient medical information. MDLive is a low acuity telehealth platform that enables patients to communicate with physicians via their smart phones, computers or other mobile devices. Without commenting on the merits of the specific claims of this case, the class action does highlight the importance of hospitals and health systems fully understanding how patient information is stored and used when coordinating telehealth services with third party providers. Not only can liability arise from unknown uses, but it also can arise when inconsistency exists between health care providers' and telehealth platform vendors' terms.

Many hospitals and health systems are currently adopting or contemplating adopting a telehealth strategy to meet community needs or as part of their telehealth strategy. To facilitate this strategy, affiliations are being adopted with direct-to-consumer telehealth platforms embedded into hospitals' or health systems' websites or mobile apps.

Due to the linking, it is often not evident to the patient that they have left the hospital's systems and have entered the independent telehealth platform's system. These independent telehealth platforms require the patient to complete a registration prior to being connected with the physician. The physician with whom the patient is connected is commonly a member of a medical practice affiliated with the telehealth vendor platform (not the underlying hospital or health system), having no affiliation or credentialing by the hospital. Telehealth platform vendors are generally not health care providers and are not covered entities under HIPAA. Rather, the telehealth platform vendor maintains a direct relationship with the patient as the licensor of the telehealth platform and as the business associate of the sponsoring hospital or health system and the physician providing the health care services.

As a condition of accessing the telehealth platform, the vendor may require that the patient consent or agree to various contractual provisions that conflict with norms established in the health care industry. Specifically, consumers may, through use of the vendor's telehealth platform, consent to the vendor's sharing with third parties any information that they have submitted to the telehealth platform (including health information) for purposes including evaluation and improvement of vendor's services, marketing, advertising and research.

Confusion can arise at various points within the telehealth visit. First, the patient may believe they are still receiving care from the hospital and/or health system and that the terms of use and privacy notice located on the hospital's or health system's website or app apply, when in fact services are being received via the independent telehealth platform and an unaffiliated clinician. Second, the telehealth platform, by considering itself as a direct-to-consumer app platform that is not a covered entity under HIPAA, may have expectations of the privacy to be provided with respect to patient-submitted information that is inconsistent with the hospital's or health system's intentions in the arrangement.

PRACTICAL TAKEAWAYS

To minimize exposure to such risk, hospitals and health systems should periodically review the operations of each telehealth platform it utilizes and assess all uses and storage of patient information. In addition, all terms and privacy notices that attach to patients seeking health care services through a telehealth platform should be reviewed to ensure they meet with the hospital's or health system's expectations and understanding of the arrangement.

If you have questions or would like additional information about this topic, please contact Mike Batt at (317) 977-1417 or mbatt@hallrender.com or your regular Hall Render attorney.