When Data Breaches Implicate Patient Care: An Evolving Legal Landscape

By: Daniel S. Marvin

Over the past several years, data breaches involving healthcare providers have become an epidemic. In fact, one recent survey reported that over 93% of healthcare organizations have experienced a data breach since Q3 2016, and 57% have had more than five data breaches during the same timeframe. Moreover, the study noted that more than 300 million records have been stolen since 2015, affecting about one in every 10 healthcare consumers. The theft of these medical records has certainly been a huge problem, both for patients who have had their records stolen and are faced with the uncertainty of how they may be used, as well as for healthcare providers which are faced with the costs and hassles of remediation. However, up until recently, the harm which could result to patients from healthcare breaches was primarily economic; that is, patients were faced with the prospects of identity theft and financial fraud. While neither of those possibilities are particularly appealing, the emergence of ransomware has drastically changed the playing field, with such attacks having the ability to completely shutter a medical provider's computer systems, thereby leaving critical information regarding patient care inaccessible, and thereby affecting patients' care.

The ability of data breaches to affect patient care is certainly not abstract. Researchers at Vanderbilt University's Owen Graduate School of Management recently took the Department of Health and Human Services (HHS) list of healthcare data breaches and analyzed patient mortality rates at more than 3,000 Medicare-certified hospitals, 10 percent of which had experienced a data breach. The results suggested that after data breaches, there were as many as 36 heart attack related deaths per 10,000 annually at the hundreds of hospitals examined, and that for care centers that experienced a breach, it took an additional 2.7 minutes for suspected heart attack patients to receive an electrocardiogram. Given these facts, it may be only a matter of time before it is commonplace for claims such as wrongful death and professional malpractice to wrangle their way into data breach related lawsuits. While we are not quite there yet, a class-action lawsuit recently filed in the United States District Court for the Northern District of Alabama is dipping its toe into the water, at least with respect to alleging impaired patient care as an element of injury. The matter is Daniels et al. v. DCH Healthcare Authority (7:19-cv-02086-LSC).

The DCH case resulted from an incident that happened over a period of 10 days in October 2019 when DCH Health System in Alabama suffered a worst-case scenario: a ransomware attack that closed the hospital system (consisting of three hospitals) down, with patients, other than the most critical, instructed to go elsewhere. On December 23, 2019, a class-action lawsuit relating to the attack followed. In the lawsuit, the plaintiffs first asserted that the ransomware attack blocked access to DCH's computer systems and data, including the highly sensitive patient

medical records and personally identifiable information of approximately 32,000 patients, and as a result, class members suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. Those types of allegations and injuries are typical in data breach class-action lawsuits, where plaintiffs generally claim that they suffered lost time and money dealing with the fallout of stolen personal information. However, what plaintiffs in DHS did next was atypical; they alleged that because of the ransomware attack, plaintiffs and class members suffered disrupted medical care, and as a result, had to: (i) find alternative medical care and treatment; (ii) delay or forego medical care and treatment; and (iii) undergo medical care and treatment without medical providers having access to a complete medical history and records.

For example, one named-plaintiff alleged that she was hospitalized and had surgery at DCH, and as a post-surgical patient suffered severe pain but, as a result of the ransomware attack, was not able to get the medications that were prescribed to her during her stay for numerous hours after her surgery. Another plaintiff -- a seven-year-old child who as an existing patient at DCH -- alleged that she sought follow-up treatment for a severe allergic reaction that caused her eyes to swell shut, but was informed that due to the ransomware attack, the hospital could not immediately see patients other than emergency room patients, and that it would be a 4-5 hour wait for treatment. Still another plaintiff alleged that when she returned to DCH during the ransomware attack, which was a week after having been treated in its emergency room (including having x-rays taken and being examined), she was told that all of her medical document files were lost or inaccessible, and as a consequence, she had to have all new x-rays taken and had to start over with her care and treatment.

The Plaintiffs in DCH asserted a claim for negligence (among other claims), and putting aside the hurdles that they may face when asserting such a claim in a data breach action, with respect to the element of injury, it is clear that the ransomware attack in this case opened up a host of potential alleged injuries other than just pure economic loss. While the alleged injuries in the DCH complaint do not appear to have been severe, as more and more devices and records in hospitals and medical offices become connected to the cloud and susceptible to cyberattack, the damage that ransomware and other attacks could potentially cause to patients is virtually limitless. The bottom line is that healthcare providers need to have a plan in place in case of a worst-case-scenario such as that suffered by DHS; as cyberattacks continue to evolve, so will the nature of claims asserted in class-action lawsuits, and so should providers' cyber resiliency. The worst thing providers can do is suffer from a failure of imagination. Rest assured, class-action plaintiffs certainly won't.