Board of Directors Medical Malpractice

2.15.2021

No, a lay member of a Board of Directors does not hold a scalpel, make an incision, diagnose a disease or otherwise render patient care, but even so is it possible for a director or an entire board to be liable for "malpractice" that could subject an institution to claims of that liability? The answer to this question is changing.

When electronic medical records were first introduced, it is not likely that many saw the exposures that we are seeing today. Whole institutions can be shut down by any one of a number of nefarious schemes by criminals and others. The battle to protect the institution from cyber intrusions is a forever thing. Billions of dollars are being spent on security for these systems which could be used for the care of patients. The decisions made in the board room and elsewhere in the institution can be decisions of life and death for a patient and possibly for the institution itself. Today, it is feasible even for an outsider to access an institution's medical records and modify a patient medical record which could have devastating effect.

To what extent can a Board of Directors or CEO be liable for such intrusions? What standard of care is required to protect the officers and directors from claims of "malpractice"? We have presented programs previously on the need for effective board governance and for appreciating and following the changing standards of care. Enterprise Cyber Risk Management is one of the key areas that have the potential for exposure to the Board of Directors and CEO. More and more board time is going to need to be devoted to the issues of cyber security. What should the CEO, Board and Risk Management be looking to in order to minimize the potential exposure? We all know that eliminating the risk entirely is not currently an option. There are, however, areas that need to be attended to and addressed by the CEO, Board and Risk Management to shield the institution from exposure and also in order to protect patients. The standard of

Related People

Robert H. Schwartz
Shareholder

Related Services

Cybersecurity and Privacy Specialty Team

Health Care

Health Care Industry Team

care will likely keep changing as the threats change but keeping up with these changes will be a key to preventing losses. The sand is not a good place to put one's head in addressing the issues of cyber risk.

So where is the guidance now? There is HIPAA of course where there are guidelines on privacy, security and breach notification. There is Office of Civil Rights (OCR) Guidance which also provides standards of care. The National Institute of Standards and Technology (NIST) also provides standards of care and is a source of publications. The NIST cybersecurity Framework was first released in 2014 and has continued to evolve.

We are seeing regulatory guidance that emphasizes the risk management role of the Board of Directors in publicly traded companies For those nonprofits and privately held institutions, the path to liability may not be as clearly defined, but can anyone believe that exposure to those boards and officers will not follow? Plaintiff litigators will continue to bring lawsuits to implicate officers and directors for breaches of their duties. At some point, it is possible they will find their mark. To address these issues and protect the board and the organization, board members should consider several steps:

- Educate the board and officers to make sure that they are aware of the issues and appropriate practices and will be able to take action in line with regulatory guidance to prevent future exposures to themselves, the institution and patients.
- For nonprofit organizations, review state law limitation on volunteer liability and update and amend articles as necessary to best implement these protections.
- Review bylaws and board policies with regard to indemnification of board members and officers who act in good faith.
- Review insurance policies that address cybersecurity, regulatory breaches, director and officer coverage, and related matters to best protect the organization and its leaders.

Our cybersecurity team has worked on many of the most significant cybersecurity matters and stands ready to assist in educating boards and executives on some of the ways to implement protection within your institution. Our healthcare and corporate attorneys have advised and trained boards on best practices in governance and compliance programs. Out attorneys also regularly advise organizations and board members on insurance coverage issues.

As noted earlier the sand is no place for one's head when addressing cybersecurity exposures. Too much is still exposed.

For assistance with these critical matters, you can contact the authors of this Alert or your Butzel attorney.

Robert Schwartz
248.258.2611
schwartzrh@butzel.com

CLIENT ALERTS

Debra Geroux
248.258.2603
geroux@butzel.com

Mark R. Lezotte
313.225.7058
lezotte@butzel.com

Jennifer Dukarski
734.213.3427
dukarski@butzel.com