STRATEGIC MANAGEMENT SERVICES

$3.5 Million Settlement by Scripps Health for Ransomware Attack Compromising Patient Information

Richard P. Kusserow | January 2023

Remember to register for the complimentary webinar "Compliance Leadership: Essential Habits, Skills, and Traits for Success," to be held Thursday, January 31, 2023, 1:00 Eastern, sponsored by SAI360.

Scripps Health settled a class action suit filed by 1.2 million individuals for negligence for failing to adequately secure and safeguard sensitive patient information. A May 1, 2021, ransomware attack crippled the Scripps' internal computer system for weeks and permitted hackers to obtain patient health information and personal financial data, and placed more than one million people at risk of identity theft. The attack caused major disruption at the Scripps hospitals, including redirecting ambulances, canceling scheduled appointments, and forcing staff to record patient information on paper for nearly a month. The data breach resulted in patients suffering lost time, annoyance, interference, and inconvenience such as not being able to access their healthcare information, request prescription refills, manage appointments, and communicate with doctors. Upon approval of the settlement agreement by the Court, a minimum of $100 will be paid to each plaintiff. Patients whose stolen identities resulted in out of pocket expenses will receive $7,500.

The suit was based upon allegations that Scripps was negligent in protecting their electronic records when it was known that cybercriminals were attacking hospitals. It was asserted that this negligence caused violations of law, including the Confidentiality of Medical Information Act and the right to privacy. The compromised information included medical history and other personal information, such as Social Security and driver's license numbers, stored on a "non-encrypted form." As a result of the attack, Scripps reported losses of $113 million in revenue for May 2021.

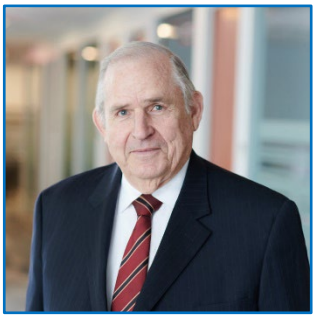
Patients who feel they were affected by the breach still have time to join in the settlement with the deadline no later than March 23, 2023. In addition, Scripps will provide credit monitoring and identity protection to all plaintiffs.

A similar suit was filed against CommonSpirit Health on December 29, 2022, alleging negligence when a ransomware attack compromised more than 600,000 patients' protected health information. As with the Scripps case, the action was based upon failure to take appropriate safeguard measures to control risks, when CommonSpirit Health should have been "on notice" of the potential risk due to similar incidents occurring in the health care industry.

A key takeaway for compliance officers is that the legal action was based upon the entities' failure to take appropriate safeguard measures to control risks when they should have been "on notice" of the potential risk due to similar incidents occurring in the health care industry. To avoid similar exposure to attacks and damages of this type, it is critical to verify and test for proper controls for protecting patient health and personal information.

Be sure to complete the 2023 Healthcare Compliance Benchmark Survey.

Keep up-to-date with Strategic Management Services by following us on LinkedIn.



About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.