STRATEGIC MANAGEMENT SERVICES

Hacking Incidents Skyrocketed During the COVID-19 Pandemic

Richard P. Kusserow | June 17, 2021

Hacking Incidents Increased by 42 Percent

A report by Protenus, Inc. indicates that that while hacking incidents in the health care industry continued to increase over the past five years, incidents increased dramatically in 2020 as organizations faced the COVID-19 pandemic. The upward trend has continued despite the adoption of and advances in health care compliance analytics.

Overall, 470 hacking incidents were reported in 2020; this represents a 42 percent increase. At least 31 million patient records were affected. Hacking incidents accounted for nearly two-thirds of health data breaches, while insider errors were responsible for 20 percent. The remainder were due to loss, theft, or unknown causes. Of the 758 data breaches reported in 2020, 492 involved health care providers (65 percent of all reporting entities), 75 involved health plans (10 percent), 94 involved a business associate (12 percent), and 97 (13 percent) involved another type of entity. Business associate incidents alone affected more than 24 million patient records.

The report also notes that health care organizations took an average of 187 days to discover that they had experienced breaches in 2020.

Reminders for Compliance

1. Ensure that a complete security risk analysis which addresses electronic protected health information (ePHI) vulnerabilities is performed at least annually.
2. Verify that Privacy and Security Officers are meeting their obligations.
3. Ensure that identified risks have been properly addressed with corrective action measures.
4. Verify that the Code of Conduct includes an expectation to report HIPAA violations.
5. Ensure that written policies and procedures outline the process to assign and retrieve laptops that provide access to ePHI.
6. Verify that controls are in place for workforce members who are provided access to ePHI.

7. Train the workforce on HIPAA policies and procedures, including the requirement to report violations.
8. Ensure that signed agreements with contact information are on file for all business associates.
9. Encrypt and password-protect all laptops and mobile devices.
10. Implement safeguards to prevent access by unauthorized users.
11. Verify the effectiveness of internal controls, policies, and procedures.
12. Assess the adequacy of security processes intended to address potential ePHI risks and vulnerabilities.
13. Ensure that the hotline is set up to receive HIPAA-related calls.

For more information on this topic, please contact Richard Kusserow at rkusserow@strategicm.com.