PLDW
HEALTH CARE

CLIENT ADVISORY:

CYBERSECURITY AND HEALTH CARE

According to the U.S. Department of Health & Human Services Office of Civil Rights, during the first six months of 2015 more than 94 million individuals were subject to security breaches at health care organizations. This is an increase of

more than 80 million individuals in 2014.[1] The average cost of a data breach in health care is $2.1 million.[2] A study by Ponemon Institute concluded that the value of an individual's health care record is between $50 and $70 mainly because the information does not grow stale and may be used over the victim's lifetime.[3] The type of health care information that is valuable to cyber criminals includes prescriptions, treatments and social security numbers.

Securing health care information is an important process for health care organizations and should commence with conducting a risk assessment to confirm that policies and procedures are in place to detect attempts at a breach. This process provides the organization with the assurance that it has the appropriate and effective response mechanisms in place. The organization should also use an independent third-party review as a check and balance to mitigate the impact of a breach and to have an established plan, policies and procedures to deal with an incident if and when it occurs.

Provider organizations and insurers are working toward implementing technologies to detect unusual transactions in order to contain the damage and appoint someone to have the exclusive authority to implement the procedures and deploy resources to address a breach. This person should be responsible for coordinating the response, determining the damage, containing the damage and addressing public relations issues. The provider should be careful to scrutinize the policies and procedures relating to cybersecurity measures by their vendors by invoking third-party reviews as well.

Encryption of data, restriction on access to data and proper levels of training of employees are essential to ensuring the proper levels of cybersecurity.

Communication between the upper level management and the security professionals is critical to the success in combating this newest level of challenges for providers. Risks may be further reduced by making certain that the policies and procedures in place are at a minimum compliant with national standards, and the provider should explore insurance coverage as another option in protecting the organizations' financial viability in the event of a breach.[4]

[1] U.S. Department of Health and Human Services Office of Civil Rights, *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf*

[2] *Cybersecurity in Healthcare: A Time To Act,* Fidelis Cybersecurity, September 2015

[3] *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data,* Ponemon Institute LLC, May 2015

[4] *Cybersecurity in Healthcare: A Time To Act,* Fidelis Cybersecurity, September 2015

GARY R. PANNONE
Managing Partner

Gary R. Pannone is the Managing Partner of Pannone Lopes Devereaux & West LLC and has been representing closely held business owners for thirty years. He is an experienced business lawyer specializing in the areas of business formations, corporate restructuring, mergers, acquisitions, corporate compliance and health care. His practice includes the representation of nonprofit organizations with respect to consolidations, mergers and acquisitions.

PLDW
PANNONE LOPES DEVEREAUX & WEST LLC
counselors at law

317 Iron Horse Way, Suite 301 Providence, RI 02908
tel 401 824 5100 • fax 401 824 5123