MURTHA MEANS
MORE
INDUSTRY INSIGHT

HEALTH CARE GROUP NEWS

August 2016

BITCOIN.
SYSTEM LOCKDOWN.
DATA HELD HOSTAGE.
RANSOM DEMAND.

If company executives are discussing the terms listed above, then their company is likely to have experienced better days. However, if the executives are in the "C Suite" or are the Compliance Officer, Privacy Officer and/or other similar individual within a health care organization, then these terms are particularly bad and come with particularly high risk.

Ransomware attacks are on the rise, up by 300% since last year, and occur 4,000 times each day. Ransomware is malicious software that has the ability to cause a computer network system lockdown, denying access to the network by encrypting the information and only providing access after a ransom is paid, commonly upwards of thousands of dollars. Ransomware frequently infects devices and systems via websites, spam, phishing messages and e-mail attachments. Infamously, earlier this year, a California hospital was the subject of a ransomware attack that disabled its electronic health record system. This hospital paid the equivalent of $17,000 in Bitcoin, the major form of electronic currency, in order to regain access to its computer systems. While a ransomware attack can wreak havoc on any business, an attack is particularly problematic for health care providers and their business associates, who require real-time access to large volumes of information in order to treat patients.

The Department of Health and Human Services, Office for Civil Rights ("OCR") recently issued new guidance on ransomware. In this guidance, OCR takes the clear position that a ransomware attack affecting protected health information ("PHI") is considered a breach of PHI under the HIPAA Breach Notification Rule, unless it can be shown, via a full HIPAA risk assessment, that there is a low probability that the PHI has been compromised. While not surprising, OCR's statement of this presumption specifically related to ransomware makes it clear that ransomware attacks are very much on OCR's radar and that, therefore, covered entities and business associates must take such attacks, and the risk of such attacks, seriously. Each health care entity and business associate should take steps to determine its ransomware-related vulnerabilities and take appropriate corrective action.

On this point, OCR advises that compliance with the HIPAA Security Rule can prevent or drastically reduce the risk of ransomware attacks. The HIPAA Security Rule requires that providers perform risk assessments of their electronic

Continued on page 2

For Questions About Health Care Matters, Please Contact:

Paul E. Knag, Co-chair
Stephanie S. Sobkowiak, Co-chair
Heather O. Berchem
Marcel J. Bernier
Frank M. Capezzera
Dena M. Castricone
Jennifer A. Corvo
Melissa A. Federico
Robert V. Giunta, Jr.
Michael C. Harrington
H. Kennedy Hudner
Daniel J. Kagan
Kenneth L. Levine
David A. Menard
Natale A. Messina
Alfred E. Smith, Jr.
Rachel Faye Smith
David R. Sullivan
Joseph R. Tarby, III
Keith S. Varian

MURTHA CULLINA LLP
ATTORNEYS AT LAW MURTHALAW.COM

BOSTON
HARTFORD
NEW HAVEN
STAMFORD
WHITE PLAINS
WOBURN

systems in an effort to identify threats and vulnerabilities to the confidentiality, integrity and availability of the electronic PHI maintained by the entity. The guidance explains how proper compliance with these requirements and the implementation of a thorough security risk management process can help to eliminate the risk of ransomware attacks. Additionally, to mitigate any harm from a ransomware attack, it is prudent for health care entities and business associates, as a part of their overall contingency plans, to maintain frequent backups of all vital data and store these backups offline and separate from the entity's main network.

When implementing any security measures, it is important to remember that the HIPAA Security Rule establishes the floor, not the ceiling, of what covered entities and business associates are required to do to safeguard the security of PHI. In the event that a health care provider or business associate experiences a ransomware attack, an appropriate response should include a timely call to experienced counsel who can help set the wheels in motion with regard to IT support, possible insurance coverage, breach reporting and contact with law enforcement if appropriate.

By Stephanie S. Sobkowiak and Daniel J. Kagan

If you have any questions regarding ransomware attacks, HIPAA breach notification or any other health law topic, please contact:

Stephanie S. Sobkowiak at (203) 772-7782 or ssobkowiak@murthalaw.com
Daniel J. Kagan at (203) 772-7726 or dkagan@murthalaw.com