SHIPMAN & GOODWIN® LLP
COUNSELORS AT LAW

HEALTH LAW
A SHIPMAN & GOODWIN® ALERT

December 12, 2014

Recent Data Breach Demonstrates the Importance of Attention to Software and IT Systems

The United States Department of Health and Human Services Office for Civil Rights ("OCR") announced that it reached a monetary settlement with an Alaskan nonprofit behavioral health care provider after the provider reported that patient health information was compromised due to malware residing on the provider's IT systems. While the OCR action was the result of the provider's potential violation of HIPAA (a health care privacy statute applicable to health care providers and health plans, and certain of their contractors), this enforcement action provides valuable insight for both health care and non-health care entities alike.

The Enforcement Action

On March 2, 2012, Anchorage Community Mental Health Services, Inc. ("ACMHS") notified OCR of a breach of the unsecured protected health information of 2,743 individuals. ACMHS determined that the breach was due to malware compromising the security of its information technology resources.

Upon notification, OCR investigated the incident and its investigation indicated that ACMHS failed to adhere to several requirements of HIPAA's security rule, including failing to conduct accurate and thorough risk assessments, failing to implement security policies and procedures and failing to implement technical security measures, such as putting firewalls in place and regularly updating software with available patches[1]. While ACHMS had adopted HIPAA policies and procedures in 2005, OCR found that they were neither fully adhered to nor updated. ACHMS settled the potential violations by agreeing to a $150,000 payment and a corrective action plan requiring ACHMS to, among other things, revise and distribute updated security policies, provide general security awareness training to staff and conduct annual risk assessments.

Health Law Practice Group:

Joan W. Feldman
(860) 251-5104
jfeldman@goodwin.com

Vincenzo Carannante
(860) 251-5096
vcarannante@goodwin.com

William J. Roberts
(860) 251-5051
wroberts@goodwin.com

www.shipmangoodwin.com

[1] A patch is a piece of software designed to update, fix or improve a computer program. For example, a patch may be used to fix security vulnerabilities.

Implications

This enforcement action has implications for virtually any business or entity that collects and maintains personal information, whether such information is health care, financial or personal (i.e. Social Security numbers) in nature. Over the last several years, such businesses have found themselves subject to an increasing number of data privacy and security laws, which, in general, impose obligations upon the businesses to protect the privacy and security of the health care, financial or personal information they maintain and to take steps to prevent the improper disclosure of such information. Because many businesses maintain such personal information in electronic format, and often on networked devices, businesses should carefully assess the measures they take to safeguard such data.

Businesses may find themselves subject to one or more of these data privacy and security laws and should seek the advice of counsel to understand and satisfy the requirements of each. While enforcement activity and penalties vary by law and state, it is safe to say that businesses face continually increasing exposure for data privacy and security liability and should be taking steps to mitigate that liability and reduce the risks of a breach. As the ACMHS matter demonstrates, data may be subject to outside attack and failure to adequately anticipate and prepare for such attacks may result in a substantial breach and significant penalties and costs. Regardless of your specific industry or the specific laws that apply to you, the following best practices will go a long way in ensuring that your data is secure and the risk of a breach is mitigated:

- Consider carefully where personal information you collect or maintain is stored or used, including computer systems, mobile devices, copiers, and cloud storage applications.
- Consider obtaining an independent risk assessment of your information technology resources to determine if such resources are sufficient to protect the privacy and security of the personal information you maintain, and to identify areas for improvement. It is often beneficial to have a fresh set of eyes.
- Prepare a work plan of immediate and long-term security improvements. Budget pressures may mean that information technology security safeguards may need to be prioritized and implemented over time. Generally, you will want to address the greatest risks, and any low-hanging fruit, first.
- Adopt policies to ensure that IT staff monitor the availability of software patches and apply those patches in a timely manner.
- Follow your policies and update them to reflect your risk assessments and changes in the law.

Resources

Fortunately, there are several resources made available to businesses by government regulators to assist with securing and protecting the personal information they collect and maintain. Some resources of general applicability include:

- The National Institute of Standards and Technology ("NIST") publishes a wide range of resources for securing data, including encryption, data transmission, data storage and securing mobile devices. Such publications are available at http://csrc.nist.gov/publications/PubsSPs.html. Of particular note in light of ACMHS is NIST's Guide for Conducting Risk Assessments available at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.
- Health care providers and health insurance companies, and vendors who provide services on their behalf involving health information (known as "business associates") are encouraged to review OCR's guidance on complying with HIPAA's security standards. Information is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html. OCR's Guidance on Risk Analysis Requirements Under the Security Rule is particularly helpful and is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.
- Businesses subject to the Gramm-Leach-Bliley Act are encouraged to review the resources provided by the Federal Trade Commission at http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

Questions?

Shipman & Goodwin offers a multi-disciplinary team of experienced lawyers who have been counseling clients on data issues for many years. We are able to provide practical, cost-effective solutions to the problems our clients face. If you have any questions about this Alert or data privacy and security in general, please contact any member of our Data Privacy and Security Team.

This communication is being circulated to Shipman & Goodwin LLP clients and friends and does not constitute an attorney client relationship. The contents are intended for informational purposes only and are not intended and should not be construed as legal advice. This may be deemed advertising under certain state laws.

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

1875 K St., NW - Suite 600
Washington, DC 20006-1251
202-469-7750

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

12 Porter Street
Lakeville, CT 06039-1809
860-435-2539

www.shipmangoodwin.com

SHIPMAN & GOODWIN® LLP
COUNSELORS AT LAW