Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

INTERNATIONAL EDITION

JANUARY 2017

IN THIS ISSUE

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

OUR AUTHORS:

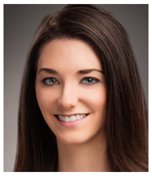
Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Laura L. Ferguson
Associate
Houston
713-226-1590
lferguson@lockelord.com

Bart W. Huffman
Partner
Austin
512-305-4746
bhuffman@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

Charles M. Salmon
Senior Counsel
Austin
512-305-4722
csalmon@lockelord.com



Ashley Wheelock
Associate
Austin
512-305-4860
ashley.wheelock@lockelord.com

Tammy Ward Woffenden
Partner
Austin
512-305-4776
twoffenden@lockelord.com

New York's Cybersecurity Requirements for DFS Licensees: A New Item at the Top of the To Do List

With a compliance date a few months away, licensees of the New York Department of Financial Services (DFS) must start taking action in response to coming cybersecurity requirements, which will be more onerous and difficult than any existing requirements in the United States. Even though the revised proposed regulation, published December 28, 2016 and available here, is open for comment until January 27, 2017, the DFS will focus on new comments that were not raised in the original comment period. As the original comment drew 150 comments addressing nearly every aspect of the proposed regulation, it is unlikely that new comments will result in further substantive changes that would justify delaying a licensee's planning. This article identifies who will be subject to the new requirements, what is required and by when, and what steps should be taken to comply.

The new requirements deserve attention from persons and companies in the banking, insurance, securities and other regulated financial industries, as it is likely that other states will look to the New York requirements as a model. The New York requirements also serve as a new and robust checklist for any business to consider for improving its cybersecurity risk profile.

I. Who is Affected?

Nearly any DFS licensee: The proposed regulation applies to Covered Entities, defined to mean each individual or non-governmental entity that operates or is required to operate under a license, registration or other authorization under the New York banking, insurance or financial services laws. There is a limited exemption from many (but not all) of the requirements for Covered Entities with fewer than 10 employees (including independent contractors), or less than $5 million in revenue in each of the past three years, or less than $10 million in assets (including affiliates). Exempt from nearly all of the requirements is any person or entity that does not directly or indirectly have any Information Systems or any Nonpublic Information. A Covered Entity that is an employee, agent, representative or designee of a Covered Entity and is covered by the cybersecurity program of the Covered Entity is exempt from the regulation. Covered Entities claiming an exemption must file a Notice of Exemption on a prescribed form.

II. What Systems and Information must be Protected?

Information Systems: Resources used to collect, process and otherwise handle electronic information, and also any specialized systems such as for industrial/process controls, telephone switching, private branch exchange and environmental control.

Nonpublic Information: Electronic information that is not publicly available, (i) the tampering with which, or unauthorized disclosure, access or use of which, would have a material adverse impact on the Covered Entity; (ii) personal information (as the term is commonly used in other privacy and security requirements); or (iii) health related information.

III. What is Required?

A. Administrative Safeguards

1. Risk Assessment. A risk assessment is required periodically, to include (i) evaluating and categorizing cybersecurity risks and threats; (ii) assessing the confidentiality and security of Information Systems and Nonpublic Information; and (iii) mitigating identified risks. While not repeated throughout this summary, and not listed first in the regulation, nearly every other administrative and technical requirement of the regulation is tied to the risk assessment.
2. Cybersecurity Program. A cybersecurity program must be designed to protect the confidentiality, integrity and availability of the Covered Entity's information systems, based on the required risk assessment, and to perform stated core cybersecurity functions.
3. Cybersecurity Policy. A cybersecurity policy approved by a senior officer or the governing board must provide for the protection of Information Systems and Nonpublic Information, based on the required risk assessment, and cover 14 specified areas including data governance and classification, systems and network security, data privacy and incident response.
4. Vendor Management. Policies and procedures must be adopted to protect the security of Information Systems and Nonpublic Information accessible to third-party vendors.
5. Personnel, Training and Monitoring. A qualified individual must be designated as the Chief Information Security Officer (CISO), responsible for the cybersecurity program and the cybersecurity policy. The CISO must report at least annually in writing to the Covered Entity's governing board concerning cybersecurity. Other cybersecurity personnel must be engaged, trained, and updated on cybersecurity risks, and all personnel must have regular cybersecurity awareness training. The Covered Entity must also implement safeguards to monitor the activity of Authorized Users and detect unauthorized access to, use of or tampering with Nonpublic Information.
6. Access Control. User access to Information Systems must be limited and periodically reviewed.
7. Application Security. All internally and externally developed applications must be secure, and procedures related to application security must be reviewed, assessed and updated periodically.
8. Testing and Auditing. Monitoring and testing of Information Systems for vulnerabilities must be conducted, including an annual penetration test and bi-annual vulnerability assessments. Systems able to reconstruct material financial transactions must be maintained. Records of Cybersecurity Events (which include unsuccessful attempts) must be maintained for five years.
9. Data Retention and Destruction. Personal information and health information no longer needed to be retained must be securely destroyed.
10. Incident Response Plan. A written incident response plan must be established to guide the response to, and recovery from, Cybersecurity Events.

B. Technical Safeguards

1. Encryption. Generally, Nonpublic Information held or transmitted by the Covered Entity must be encrypted, both in transit and at rest. To the extent that encryption is determined to be infeasible, alternative compensating controls may be substituted, subject to review by the CISO at least annually.

2. Multi-Factor Authentication. To protect against unauthorized access to Nonpublic Information or Information Systems, each Covered Entity must use Multi-Factor Authentication or Risk-Based Authentication (as these terms are defined in the regulation). As an alternative, the CISO can approve other access controls that are at least as secure.

C. Notices

1. Breach Notices. Notice is required to the DFS superintendent as promptly as possible but no later than 72 hours from a determination that a Cybersecurity Event has occurred, where notice is required to any other governmental or supervisory body, or self-regulatory agency or where the event has a reasonable likelihood of materially harming any material part of the Covered Entity's operations.

2. Annual Compliance Certification. An annual compliance certification on the prescribed form must be submitted to the DFS superintendent by February 15 of each year, starting in 2018. Documentation supporting the certificate must be maintained for examination by the DFS for five years.

3. Confidentiality. All information provided by a Covered Entity pursuant to the regulation is exempt from disclosure under public records laws.

IV. When are the New Requirements Effective?

The regulation will be effective March 1, 2017, and Covered Entities will have until September 1 to comply. The following listing indicates the actual compliance date for the various requirements, given the separate deadline for the annual compliance certificate, and three different transition periods of the regulation.

Compliance Date	Provision (with Regulation Section reference)
September 1, 2017	Cybersecurity Program (§ 500.02) Cybersecurity Policy (§ 500.03) CISO (§ 500.04(a)) Access Privileges (§ 500.07) Cybersecurity Personnel (§ 500.10) Incident Response Plan (§ 500.16) Notice of Cybersecurity Event (§ 500.17(a)) Filing for Limited Exemption (§ 500.19(d))
February 1, 2018	Annual Compliance Certification (§ 500.17(b))
March 1, 2018	CISO's annual report to the governing board (§ 500.04(b)) Pen Testing and Vulnerability Assessments (§ 500.05) Risk Assessment (§ 500.09) Multifactor Authentication (§ 500.12) Cybersecurity Awareness Training for all Personnel (§ 500.14(a)(2))
January 1, 2019	Audit Trail (§ 500.06) Application Security (§ 500.08) Data Retention Limits (§ 500.13) Monitoring and Detection of activity of Authorized Users (§ 500.14(a)(1)) Encryption (§ 500.15)
March 1, 2019	Third Party Vendor Security (§ 500.11)

V. What Steps should be Taken?

Each Covered Entity should start now to review existing programs, policies and procedures to determine what is needed to satisfy the new requirements by the compliance dates mapped above. It is difficult to imagine any Covered Entity that would not have to take some action to comply with the new requirements. The following project steps are suggested for consideration by Covered Entities:

1. Determine whether or not the limited exemption for small businesses, or one of the other exemptions, would apply.

2. Identify and gather the project team, consisting of internal decision makers, IT personnel and internal and experienced external legal and regulatory resources.

3. Identify outside resources that will be required for various functions, such as pen testing.

4. Catalogue all existing programs, policies and procedures related to cybersecurity.

5. Assign team members responsible for reviewing and, as necessary, revising each existing program, policy and procedure, and to draft any new documentation needed to comply with the new requirements.

6. Map the timeline of deliverables to achieve compliance by the effective date and the various transition dates.

New Year, New Rules – The 2017 Illinois Personal Information Protection Act

On January 1, 2017, Illinois ushered in a broader and stronger personal information and data breach regime. The Illinois Personal Information Act (PIPA), 815 ILCS § 530, applies to any entity that "handles, collects, disseminates, or otherwise deals with nonpublic personal information," and imposes certain obligations on those entities in the event of a breach of Illinois residents' "personal information." The changes run throughout the law, with key revisions or additions including:

- Definition of "personal information": the definition grew in two ways. First, the definition as tied to a person's name and some other identifying information was expanded to mean a person's first name or initial and their last name along with certain details such as a Social Security number, when such information is not encrypted or redacted or when the access to the shielded information has been hacked. In addition, the list of identifying details has grown to include medical information, health insurance information and "unique biometric data" such as a fingerprint. Second, a new definition of "personal information" was added to concern a person's "user name or email address, in combination with a password or security question and answer that would permit access to an online account," with the same new language about encryption and redaction as in the first definition. 815 ILCS § 530/5.

- Notice of breach: the notice obligation was amended to address the new online account definition of "personal information." When the breach concerns this type of personal information, "notice may be provided in electronic or other form" and is to direct the Illinois resident "to promptly change" the information that has been breached for not only the resident's account identified by the entity providing notice but also all other accounts for which the resident uses the same user name, password or security question and answer. 815 ILCS § 530/10.
- Data Security requirements: A new section extends to any entity covered by the Act that "owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident." Under the amended Act, such an entity "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." 815 ILCS § 530/45(a). In addition, if an entity has a contract for the disclosure of such information, it must specify that the person obtaining the information must also maintain such security measures. 815 ILCS § 530/45(b). The Act confirms that an entity's compliance with an applicable state or federal law (including the Gramm-Leach-Bliley Act of 1999) that calls for "greater protection" constitutes compliance with the Act. 815 ILCS § 530/45(c) and (d). As to entities subject to the federal Health Insurance Portability and Accountability Act of 1995 and the Health Information Technology for Economic and Clinical Health Act, the Act says that compliance with those federal laws is sufficient so long as notification of a breach made to the Secretary of Health and Human Services is also given to the state Attorney General within five business days thereafter. 815 ILCS § 530/50.

DHS Releases Strategic Principles for Security of the Internet of Things

On November 15, 2016 the U.S. Department of Homeland Security released its Strategic Principles for Security of the Internet of Things (IoT) (the "Strategic Principles"). DHS recognizes that rapid innovation in the IoT may provide tremendous benefits, but that "IoT security, . . . has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks." The Strategic Principles are designed to explain risks and suggest best practices "to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate."

The Strategic Principles speak to an audience of IoT stakeholders, comprised of IoT developers, IoT manufacturers, service providers dependent on IoT and industrial and business-level consumers. According to DHS, IoT stakeholders should, as applicable:

- incorporate security at the design phase and enable security-by-default, to allow for increased security and avoid unnecessary costs of fixing problems later;
- promote security updates and vulnerability management, including use of automation to provide updates and patches seamlessly;
- building on recognized security practices, including security for software design as well as sector-specific guidance;
- prioritize security controls and other measures according to potential impact, taking into account:
  - practical considerations, such as the intended environment for an IoT device's use; and
  - "red teaming" to assess the threat level posed by more serious risks;
- promote transparency across IoT design and implementation, including full life cycle and evaluation of third-party practices; and
- connect carefully and deliberately, considering whether and how:
  - users should be advised of the purpose of IoT connections; and
  - additional controls should be included to address the existing and foreseen connection possibilities.

Consistent with the objectives of the Strategic Principles, DHS indicates that policymakers need to continue to evaluate and understand risks and to work on incentives for appropriately securing the IoT. Like the NIST Cybersecurity Framework, the Strategic Principles are not intended to provide strict requirements, but instead to provide "a risk-based approach that takes into account relevant business contexts." Although standard-setting and regulatory efforts for the IoT are still in their infancy, the Strategic Principles provide helpful insights and framework for IoT stakeholders.

After the Fact: FDA's Guidance on Postmarket Management of Cybersecurity in Medical Devices

The Food and Drug Administration (FDA) recently issued nonbinding guidance focusing on the software vulnerabilities of networked medical devices that are already on the market. The postmarket management guidance is available here. The guidance focuses on the importance of detecting (and correcting, if possible) the inadvertent incorporation of vulnerabilities during the design and manufacture of medical devices (which is the subject of separate guidance available here).

The FDA recommends that a manufacturer implement a cybersecurity risk management program that is consistent with the Quality System Regulation (21 C.F.R. part 820) and incorporate elements consistent with the NIST Framework for Improving Critical Infrastructure Cybersecurity. An appendix to the postmarket guidance lays out the elements of an effective postmarket cybersecurity program, to be used in a manner consistent with the NIST Framework, as follows:

- Identify (maintaining safety and essential performance, and identification of cybersecurity signals);
- Protect/Detect (vulnerability characterization and assessment, risk analysis and threat modeling, analysis of threat sources, incorporation of threat detection capabilities and impact assessments);
- Protect/Respond/Recover (compensating controls assessment); and
- Risk Mitigation of Safety and Essential Performance.

The postmarket guidance also establishes a risk-based framework for assessing when to report (or not to report) to the FDA about a change to be made as a result of a cybersecurity vulnerability. For example, the FDA clarifies that routine cybersecurity updates and patches do not need to be reported to the FDA in advance, whereas reporting is required when patient harm may result from the vulnerability. The FDA stresses that "[t]he presence of a vulnerability does not necessarily trigger patient harm concerns. Rather it is the impact of the vulnerability on the safety and essential performance of the device which may present a risk of patient harm." Manufacturers of networked medical devices should review the postmarket guidance against the manufacturer's current cybersecurity program to ensure that it is addressing the FDA's concerns or whether tweaks to the program should be made in light of this guidance.

Department of Energy Raises Concerns on Cybersecurity for Grid

The U.S. Department of Energy has raised serious concerns regarding cybersecurity vulnerabilities within the U.S. energy grid in its Quadrennial Energy Review. Chapter IV of the Review (which begins on its 272nd page) "addresses a range of possible risks to the electricity system and the broader economy, and it suggests options to mitigate and prepare for these risks."

The Review paints an ominous picture of the cybersecurity challenges on the horizon for those protecting the grid, stating:

> In the current environment, the U.S. grid faces imminent danger from cyber attacks. Widespread disruption of electric service because of a transmission failure initiated by a cyber attack at various points of entry could undermine U.S. lifeline networks, critical defense infrastructure, and much of the economy; it could also endanger the health and safety of millions of citizens. Also, natural gas plays an increasingly important role as fuel for the Nation's electricity system; a gas pipeline outage or malfunction due to a cyber attack could affect not only pipeline and related infrastructures, but also the reliability of the Nation's electricity system.
>
> (Emphasis added.)

Several recommendations are made to policymakers with respect to how to address these challenges, including:

- amendment to the Federal Power Act to "clarify and affirm the Department of Energy's [] authority to develop preparation and response capabilities";
- collection of targeted data by DOE to report to the President concerning vulnerabilities and actions to be take in response to those vulnerabilities;
- adoption by the Federal Energy Regulatory Commission of "standards requiring integrated electricity security planning on a regional basis" (to the extent consistent with statutory authority); and
- assessment of natural gas infrastructure to determine if additional protections are needed.

In the words of the Report, the "era of enhanced grid operations through artificial intelligence is here." However, proper execution using new technologies "must occur in a context that assiduously assures deflection of cyber attacks that could cripple grids; it must also occur through market mechanisms to help value and ensure cost-effective outcomes." These statements make clear that U.S. regulators continue recognize both the vulnerabilities and critical nature of the energy grid. Those involved with energy grid management, or those with significant ties to or dependencies on related entities, should remain watchful of updates to cybersecurity threats and requirements.

Ransomware? Everywhere!

The definition of "ransomware" can sound pretty academic. For example, the FBI describes ransomware as "a type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid." However, the reality of ransomware is anything but textbook. It can hobble an organization's operations, create financial loss, risk injury and more. Fortunately, there are some important steps an entity can take to reduce its risk, including considering insurance.

The nefarious practice of ransomware affects entities of all types and sizes. And business is booming for these attackers. According to a recent SentinelOne survey, about 50% of businesses suffered a ransomware attack in the last 12 months. "Ransomware has become one of the most successful forms of cybercrime in 2016 and is on the top of every security professional's list of most prolific threats," declares Jeremiah Grossman, chief of security strategy at SentinelOne. U.S. government statistics show "ransomware attacks quadrupled in 2016, with an average of 4,000 attacks per day."

The FBI "does not support paying a ransom to the adversary," contending there is no certainty access will be returned. In addition, the FBI cautions that "[p]aying a ransom emboldens the adversary to target other victims for profit . . ." The attacks are lucrative. As noted by a recent IBM Security Survey, "[t]he FBI reported that in just the first three months of 2016, more than $209 million in ransomware payments have been made in the United States – a dramatic 771 percent increase over a reported $24 million for the whole of 2015. The FBI estimates ransomware is on pace to be a $1 billion dollar source of income for cybercriminals [in 2016]."

Those significant figures are the totals from ransoms that are currently individually small or fairly modest. While information varies, the IBM Survey references an average ransom demand of $500. There have been publicized exceptions, with demands even in the millions and with actual payments of "4- to 5-digit" ransoms. As the assaults mature, twists are emerging. SentinelOne cites the risk of perpetrators demanding a second ransom payment after receipt of the first. In addition, they describe the threat and perhaps the real risk of having materials leaked online if a ransom is not paid. Another variation is referred to as "Popcorn Time," in which the attackers ask for payment, but also offer the alternative of a return of access for free if the victim agrees to send a malicious link to two or more people, serving up new prey to the attackers.

As ransomware gains momentum, some observers discuss whether the practice will get more sophisticated and possibly more expensive or whether it will cannibalize itself if other less-disciplined hackers swarm in. The tension is between current success with modest ransoms followed by returned access and the prospect of much larger ransoms without a guarantee the attackers honor the deals. The former could be self-sustaining, with it being cheaper for most entities to just pay. The latter could particularly motivate entities and law enforcement to refuse to pay. Regardless, cybersecurity company McAfee Labs foresees that there will be more technological and legal measures that could reduce the number and extent of such attacks.

Entities do have options. Experts stress the importance of backing up data frequently, considering isolating key information on a separate system, training employees to prevent introduction of ransomware, maintaining current virus protection programs, developing a ransom response plan and more. While these steps may not be foolproof, they may reduce the risk of penetration and decrease the impact of losing access temporarily or permanently.

One additional measure is to evaluate purchasing insurance. Organizations should discuss this option with their risk managers or other relevant staff and with a knowledgeable insurance broker. Various insurers offer differing products that may cover, for example, a ransom, investigation costs, response costs or other sums, subject to the terms and conditions of the policy. The amount of the applicable deductible and available limits also varies. The underwriting process may include a review of and possibly requirements for a potential insured's preparedness to identify and respond to a ransomware attack. Such policies likely require consent by the insurer before any ransom is paid. In addition, the policyholder may have to agree not to publicly disclose it has such insurance.

NIST Releases Draft Update to Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has released its first draft update (the "Draft Update," available with and without markup here) to its 2014 Framework for Improving Critical Infrastructure Cybersecurity. The Framework was designed to provide guidance for organizations seeking to enhance cybersecurity relating to critical infrastructure, and has been used by a broad array of organizations to define and achieve cybersecurity goals. The Draft Update was prepared to "refine" the Framework and make it easier to use, according to Matt Barrett, NIST's program manager for the Cybersecurity Framework.

Release of the Draft Update is made in consideration of comments received by NIST in the years since promulgation of the Framework. The Draft Update revises the Framework to provide additional guidance on addressing supply chain risks and cybersecurity measurement and demonstration methods.

On the topic of supply chain risk management, the Draft Update identifies a primary consideration as "assess[ment] and mitigat[ion] of 'products and services that may contain potentially malicious functionality, are counterfeit or are vulnerable due to poor manufacturing and development practices within the cyber supply chain.'" (Citing NIST Special Publication 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.) On this issue, the Draft Update includes guidance on:

- the establishment of security requirements for suppliers (with appropriate communications, enforcement and validation protocols);
- consideration of cybersecurity issues in buying decisions; and
- means to assess supply chain risk management within the Framework's traditional Implementation Tiers.

With respect to cybersecurity measurement methods, the Draft Update sets forth a reasonable, realistic approach to cybersecurity measurement, recognizing the needs for effective management of costs, and to correlate cybersecurity measures to business needs. The Draft Update goes on to provide a table of "Types of Framework Measurement" for organizations, including through Practices ("General risk management and behaviors"); Process ("Specific risk management activities"); Management ("Fulfillment of general cybersecurity outcomes"); and Technical ("Achievement of specific cybersecurity outcomes").

A NIST release concerning the update is available here. The Draft Update is subject to public comment through April 10, 2017, and comments may be submitted to cyberframework@nist.gov. The Framework remains a practical, risk-based guidance document for entities seeking to improve their information security practices, and, as noted by Mr. Barret, "voluntary and flexible to adaptation."

HIPAA Enforcement Update (October 2016 – January 2017)

Since October 2016, the Department of Health and Human Services, Office for Civil Rights (OCR) announced four settlement agreements to resolve allegations of Health Insurance Portability and Accountability Act (HIPAA) violations. These settlements are consistent with OCR's recent pattern of increased HIPAA enforcement activity, steep penalty assessments and low tolerance for failure to fully implement and comply with requirements of the HIPAA Privacy, Security and Breach Notification Rules.

Most recently, on January 18, 2017 OCR announced a $2.2 million settlement agreement underscoring the need for covered entities to implement safeguards for electronic protected health information (ePHI). Here, MAPFRE Life Insurance Company of Puerto Rico (MAPFRE) filed a breach report with OCR indicating that a USB data storage device containing ePHI of 2,209 individuals was stolen from its IT department. During OCR's subsequent investigation, it found MAPFRE failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI, and MAPFRE had not implemented security measures, such as encryption, sufficient to reduce risks and vulnerabilities to a reasonable level. This settlement agreement serves as a reminder to covered entities and business associates that—as required by the HIPAA Security Rule—they must conduct enterprise-wide risk analyses of ePHI security, develop a risk management plan addressing and mitigate any security vulnerabilities identified.

On January 10, 2017, OCR issued a press release announcing its first HIPAA settlement agreement for the untimely reporting of a breach of unsecured protected health information (PHI). Presence Health, a non-profit health care system in Illinois, sustained a data breach on October 22, 2013 when it could not locate its paper-based operating room schedules containing the PHI of 836 individuals. During the course of its investigation, OCR discovered that Presence Health failed to provide notification of the breach within the timeframes outlined in the HIPAA Breach Notification Rule. In this case, Presence Health should have provided notification of the breach to affected individuals, prominent media outlets and OCR without unreasonable delay and no later than 60 calendar days after its discovery of the breach. However, Presence Health provided notifications to individuals and the media 104 calendar days following discovery of the breach and notified OCR 101 calendar days after discovering the breach. Presence Health's failure to notify the 836 affected individuals each constituted a separate violation of the Breach Notification Rule, 45 C.F.R. 164.404(b). Under the terms of the settlement agreement, Presence Health agreed to pay $475,000. Importantly, this settlement signals OCR's intention to enforce breach notification deadlines, and covered entities and business associates must be mindful of reporting timelines or risk potential violations.

On November 22, 2016, OCR announced a resolution agreement with the University of Massachusetts Amherst (UMass), emphasizing the necessity for an entity to correctly designate all of its health care components when electing "hybrid entity" status under HIPAA. Here, an impermissible disclosure of 1,670 individuals' ePHI occurred when a workstation in UMass's Center for Language, Speech, and Hearing (the "Center") was infected with malware in 2013. During OCR's investigation, it learned that UMass incorrectly determined that the Center was not a health care covered component within its hybrid entity designation and, consequently, had not implemented HIPAA-compliant policies and procedures at the Center. OCR entered into a settlement agreement requiring UMass to pay $650,000. OCR noted in the settlement agreement that, when determining the settlement amount, it took into consideration the fact that the University operated at a financial loss in 2015 and that the Center provides unique services to an underserved population. This settlement emphasizes the importance of a hybrid entity conducting a full evaluation of all of its operations in order to properly identify which of its functions and departments are health care components subject to HIPAA regulation.

Lastly, on October 17, 2016, St. Joseph Health (SJH) entered into a settlement agreement with OCR requiring it to pay a $2,140,500 penalty. In this matter, SJH purchased a server with a file sharing application that defaulted to give file access to anyone with an Internet connection. Upon implementation of this server and the file sharing application, SJH did not examine or modify the default settings. As a result, the public had unrestricted access to PDF files containing the ePHI of 31,800 individuals, including patient names, health statuses, diagnoses and demographic information. This settlement emphasizes the need for an entity to thoroughly understand all of its technology equipment and security settings. Entities must not only conduct a comprehensive risk analysis but must also evaluate and address potential security risks when implementing enterprise changes impacting ePHI.

Locke Lord LLP

Practical Wisdom, Trusted Advice.

www.lockelord.com

Atlanta | Austin | Boston | Chicago | Cincinnati | Dallas | Hartford | Hong Kong | Houston | London | Los Angeles | Miami
Morristown | New Orleans | New York | Providence | Sacramento | San Francisco | Stamford | Washington DC | West Palm Beach

Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This brochure is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice. If you would like to be removed from our mailing list, please contact us at either unsubscribe@lockelord.com or Locke Lord LLP, 111 South Wacker Drive, Chicago, Illinois 60606, Attention: Marketing. If we are not so advised, you will continue to receive brochures. (012417)