

# **Converging Headwinds for Cybersecurity: New Regulatory Mandates, Patient-Driven Care, and Big Data for Population Health Management**

**Jack Wolf**

Senior Vice President & Chief Information Officer,  
Montefiore Health System

**Tracy Miller, Esq.**

Bond, Schoeneck & King PLLC



Health Law Section Program  
New York State Bar Association Annual Meeting  
January 16, 2019

Session:      Converging Headwinds for Cybersecurity: New Regulatory Mandates, Patient-Driven Care, and Big Data for Population Health Management

Speakers:     Jack Wolf, Senior Vice President & Chief Information Officer, Montefiore Health System

Tracy Miller, Esq., Member, Bond, Schoeneck & King, PLLC

Materials for Session:

1.      “Deadline Approaches For Major Requirements Under New York’s Cybersecurity Rule,” Tracy E. Miller and Curtis A. Johnson, Bond Information Memo, August 28, 2018.
2.      “NY Cybersecurity Regulations Will Affect Health Care Sector,” Tracy E. Miller, Law360, March 20, 2017.
3.      “European Privacy Regulation Will Impact U.S. Health Care Organizations,” Tracy E. Miller and Robert W. Patterson, Bond Information Memo, May 17, 2018.
4.      “Employers May Be Liable for the Release of Employees’ Personally Identifying Information in Data Breaches,” Nicholas P. Jacobson, Bond Information Memo, December 6, 2018.

## Deadline Approaches for Major New Requirements under New York's Cybersecurity Rule

New York's cybersecurity regulations ("Regulations") set forth rolling deadlines, with some of the most significant mandates coming into play on September 1, 2018. Issued by the Department of Financial Services ("DFS"), and effective on March 2017, the Regulations apply to all entities licensed or regulated by DFS, including but not limited to banks, mortgage lenders, insurance companies and health plans in New York State ("Covered Entities").

### General Requirements

Overall, the Regulations, among the most prescriptive in the nation, require Covered Entities to:

- Adopt a written cybersecurity policy setting forth policies and procedures for the protection of their information systems and broadly defined nonpublic information protected under the Regulations ("Nonpublic Information");
- Designate a qualified individual to serve as Chief Information Security Officer responsible for overseeing, implementing, and enforcing the cybersecurity program and policy; and
- Adopt policies and procedures designed to ensure the security of Nonpublic Information accessible to, or held by, third parties.

### The New Mandates

The specific requirements that must be in met by September 1 are as follows:

- **Audit Trail** – Covered Entities must begin to maintain an audit trail that allows them to reconstruct material financial transactions to support normal operations in the event of a breach. Audit trails must also be useful in detecting and responding to cybersecurity events. Audit trail records permitting the reconstruction of financial transactions must be maintained for 5 years and those used to detect and respond to cybersecurity events must be kept for 3 years. (23 N.Y.C.R.R. § 500.06)
- **Application Security** – Covered Entities' cybersecurity programs must now include written procedures, guidelines and standards for the in-house development of software and procedures for testing the security of externally developed applications. (23 N.Y.C.R.R. § 500.08)
- **Limitations of Data Retention** – Covered Entities must adopt procedures for the periodic disposal of Nonpublic Information that is no longer necessary for business operations or other legitimate purposes of the Covered Entity, except where that information must otherwise be maintained by law or regulation or where targeted disposal is not reasonably feasible due to the manner of maintaining the information. (23 N.Y.C.R.R. § 500.13)
- **Monitoring** – Covered Entities must implement risk-based policies and controls designed to monitor activities of authorized users to detect unauthorized access, use of or tampering with Nonpublic Information by authorized users. (23 N.Y.C.R.R. § 500.14(a))

- **Training** – Covered Entities must provide regular cybersecurity awareness training for all personnel, updated as necessary to reflect risks identified by the Covered Entity in its periodic risk assessments. (23 N.Y.C.R.R. § 500.14(a))
- **Encryption of Nonpublic Information** – Nonpublic Information must now be encrypted both in transit and at rest, however alternative compensating measures are permitted where encryption is not feasible. (23 N.Y.C.R.R. § 500.15)

### **Breadth of the Encryption Requirement**

The encryption requirement is broad and applies to all Nonpublic Information in a Covered Entity's possession. The Regulations define Nonpublic Information as:

1. Business-related information of a Covered Entity which if tampered with, or subject to unauthorized disclosure, access or use, would cause a material adverse impact to the business, operations, or security of the Covered Entity;
2. Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;
3. Any information or data, except age or gender, in any form or medium, created by or derived from a health care provider or an individual and that relates to: (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual. (23 N.Y.C.R.R. § 500.01(g))

Covered Entities must determine what data falls into the first category of Nonpublic Information based on their risk assessments. Nonpublic Information as defined above in the latter two categories must be encrypted. However, the regulations permit the Chief Information Security Officer to authorize effective alternative compensating controls for the Covered Entity, where encryption would not be feasible.

### **Certification of Compliance**

On February 15, 2018, Covered Entities were required to certify to DFS that they were in compliance with those portions of the Regulations then in effect. The next annual certification deadline is February 15, 2019. A Covered Entity's board of directors, or a senior officer, will be required to execute a certificate of compliance on or before that date which certifies compliance with each applicable requirement of the Regulations.

### **Limited Exemptions May Apply to New Mandates**

The requirements that become effective under the Regulations on September 1 are among the most challenging, costly, and demanding to implement. For example, encryption requires in the first instance the identification of all Nonpublic Information transmitted and stored by the Covered Entity. Audit trails must be targeted based on the risk assessment and should be established to yield the information that organizations need both to detect an intruder and track access in the wake of a breach. Small Covered Entities—those with fewer than 10 employees, less than \$5 million in gross annual revenue or less than \$10 million in assets—can apply for a limited exemption. Under the limited exemption, small Covered Entities are still bound by the data retention provision of the new mandates, but not the encryption, audit trail, application security, and monitoring requirements. (23 N.Y.C.R.R. § 500.19(a))

### **On the Horizon – Oversight of Third Party Service Providers**

Under the Regulations, Covered Entities will soon be required to implement written policies and procedures governing their practices with respect to third party service providers that access Nonpublic Information ("Contractors") based on the Covered Entity's risk assessment. Specifically, as set forth in the Regulations, Covered Entities must adopt policies that address:

- Identification and risk assessment of Contractors;
- Minimum security practices that must be met by Contractors in order to do business with the Covered Entity;
- Procedures for due diligence to evaluate the adequacy of Contractors' security practices; and
- Guidelines for contractual protections relating to Contractors' access to Nonpublic Information.

Consistent with a risk assessment by the Covered Entity, such policies must address Contractors' procedures for access control, including multi-factor identification, encryption of information in transit and at rest, and practices to notify the Covered Entity of a cybersecurity event that directly impacts the Covered Entity's information systems and Nonpublic Information. Guidelines must also cover the representations and warranties that Contractors will extend to the Covered Entity regarding their cybersecurity policies.

For questions about the Cybersecurity Rule and steps required to achieve compliance, contact Tracy Miller, Co-Chair Cybersecurity and Data Privacy Practice Group or Curtis Johnson.

**Tracy E. Miller**  
(tmiller@bsk.com)

**Curtis Johnson**  
(cjohnson@bsk.com)

## NY Cybersecurity Regulations Will Affect Health Care Sector

Law360, New York (March 20, 2017, 1:23 PM EDT) -- Designed for banks, insurance companies and other financial institutions, New York state's regulations, effective as of March 1, 2017, adopted sweeping new requirements for cybersecurity programs. The regulations established a broad footprint, not only in terms of the obligations imposed, but in the scope of organizations covered. In response to public criticism, the New York State Department of Financial Services revised the regulations somewhat, principally by tying certain elements of the mandated cybersecurity program to a risk assessment by each covered entity. Nonetheless, the regulations remain far more prescriptive than preceding regulatory schemes, including the security requirements of the Health Insurance Portability and Accountability Act that have long applied to the health care sector.[1] As a result, the cybersecurity regulations can be expected to have wide impact outside the arena of financial institutions in New York state.



Tracy E. Miller

The regulations apply to all organizations that operate under a license, permit, registration, charter, certificate, accreditation or similar authorization under the New York Banking Law, Insurance Law or Financial Services Law, unless an exemption applies. Health insurance companies and health maintenance organizations regulated by DFS (health plans) are therefore covered entities under the regulations. As such, they must adopt a cybersecurity program that meets the required specifications of the regulations, with a written policy that covers security measures for all "nonpublic information," including the management of third-party service providers. Given the stringent requirements for third parties in the regulations, health care providers will also face significant new obligations as health plans move to comply with the third-party contracting requirements.

While revised in the final regulations, the requirements for third-party contractors remain exacting. Among other obligations, covered entities must:

- Identify and assess the risk posed by third-party contractors;
- Set minimum standards for the security practices of third parties with whom they do business;
- Adopt due diligence processes to evaluate third-party security practices; and
- Periodically assess third-party contractors based on the risk they present to nonpublic covered information, defined to include medical information.

### Beyond the Demands of HIPAA

One of the earliest body of regulations governing cybersecurity, the HIPAA Security Rule is scalable and flexible; it does not specify technology requirements, with the exception of the standards for encryption that must be met to determine whether a breach has occurred and must be reported. Under the HIPAA Security Rule, security measures must be reasonable in light of the size and capabilities of each organization, recognizing that the security needs and capacity of covered entities vary considerably in the health care sector.

The New York cybersecurity regulations depart from this approach, enumerating technical safeguards and standards that must be considered or adopted, including continuous monitoring

or annual penetration testing and biannual vulnerability assessment, and encryption for nonpublic information not only in transmission, but at rest. Consistent with a risk assessment, covered entities must adopt policies for third-party contractors that address procedures for access control, including multifactor identification, encryption of information in transit and at rest, and representations and warranties that contractors will extend to the covered entity regarding their cybersecurity policies and practices. HIPAA requires covered entities to bind third parties that will receive protected health information to comply with HIPAA in a business associate agreement. While those agreements may specify security safeguards, HIPAA does not mandate technical safeguards or solutions that must be encompassed in the agreements.

The requirements for breach reporting under the New York regulations are also distinct from HIPAA, but are tied in part to the duty to report under HIPAA's breach notification rule. In accordance with HIPAA, entities must report a breach of unsecured protected health information to the secretary of the U.S. Department of Health and Human Services, without unreasonable delay, but no later than 60 days following a breach that affects 500 or more individuals. Covered entities must also notify affected individuals in the same time frame, providing the information as required by the breach notification rule.<sup>[2]</sup> HIPAA enumerates exceptions to reporting, including instances where the covered entity determines that there is a low probability that the protected health information was compromised based on a risk assessment. The New York regulations require a report to DFS as promptly as possible, but in no event later than 72 hours from a determination that: (1) an event has occurred that has a reasonable likelihood of harming any material part of the normal operations of the covered entity; or (2) the entity must report to another governmental or supervisory body. The obligation to report and the time frame for reporting to DFS under the second criteria are therefore dependent on the assessment and determination by health plans of the duty to report to HHS as required by HIPAA.

The New York regulations allow two years for covered entities to implement the third-party contracting requirements. As health plans adopt and implement their policies, health care providers will be subject to differing standards, in a regulatory scheme that focuses on technical solutions rather than the size or capability of organizations. For that reason, New York's regulations may prove particularly problematic for smaller health care providers. A wide array of health care providers are now engaged in data exchange in New York state to carry out value-based payment driven by public and private payers. New York state has invested \$8 billion to transform care delivery in the Medicaid program, by fostering the development of networks comprised of hundreds of health care providers, spanning the spectrum from large hospital systems to physician practices, behavioral health and home care providers. New York's cybersecurity regulations are likely to drive up the cost of participation in these arrangements, with the biggest impact on smaller providers across the continuum of care. The two-year lag in the implementation date of the third-party contract provisions will provide some relief, but implementation is still likely to prove costly and complex for many health care providers.

### **Reprieve for Universities, Colleges, and Other Not-for-Profit Organizations**

As proposed in September and again in December 2016, the New York regulations would have applied to all organizations in the state that hold a permit from DFS. Many colleges and universities as well as hundreds of other not-for-profit organizations have a permit for a donor annuity program from DFS, ranging from some of the largest museums and other cultural institutions in the state to major universities, social services agencies, religious organizations, and foundations. The proposed regulations would have required these organizations to adopt the stringent security standards set forth in the regulations across the information systems and the diverse types of private information they maintain. In many cases, banks manage the donor annuity program and hold the private financial information for donor annuity clients, further undermining the rationale for bringing not-for-profit organizations under the ambit of the regulations.

Public comments urged that covering these organizations would impose a costly burden, with a regulatory scheme unrelated to their mission, size and resources.<sup>[3]</sup> While DFS had signaled that the final regulations were unlikely to embody significant changes, the final regulations exempt organizations covered solely because they hold a donor annuity program permit, relieving universities, colleges, and other not-for-profit organizations in the state of the burden of complying with the demanding regulations crafted for the financial sector.



*Tracy Miller is a partner in Bond Schoeneck's New York office. She co-chairs the firm's cybersecurity and data privacy practice, and is deputy chairwoman of the health care and long-term care practice.*

*The opinions expressed are those of the author and do not necessarily reflect the views of the firm or its clients. This article is intended for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] HIPAA Security Rule, 45 CFR Part 160 and 45 CFR Part 164, Subparts A and C.

[2] 45 CFR § 164-400-414.

[3] Letter to Cassandra Lentchner, by Tracy Miller, joined by the New York Commission on Independent Colleges and Universities, January 27, 2017.

All Content © 2003-2017, Portfolio Media, Inc.

## European Privacy Regulation Will Impact U.S. Health Care Organizations

Effective May 25, 2018, the European General Data Protection Regulation ("GDPR") imposes new obligations on persons or entities that are "controllers" or "processors" of "personal data" about individuals in the European Union ("EU"). Unlike U.S. or even current privacy laws in Europe, the GDPR: (i) can apply to entities that are located *entirely outside* of the EU; and (ii) applies to personal data about *anyone in the EU*, regardless of whether they are a citizen or permanent resident of an EU member state.<sup>2</sup> As a result, the GDPR has significant extraterritorial reach.

The GDPR covers "personal data" defined broadly to include information that identifies or is identifiable about an individual, including health care, financial, and social information ("Personal Data"). U.S. health care providers and institutions – including health systems, health plans, academic medical centers, hospitals, physicians, payers, nursing homes, and alcohol and drug treatment centers – will be subject to the GDPR if they have the requisite relationship to Personal Data about individuals in the EU, directly or through vendors or contractors. For example, the GDPR could apply to U.S. health care providers and institutions that:

- Treat patients in the EU in-person or remotely via telemedicine, teleradiology or other means;
- Continue to monitor EU patients after they are treated in the U.S.;
- Conduct clinical programs involving data subjects in the EU, including through health care facilities located either in the U.S. or the EU;
- Employ providers or staff from the EU who provide Personal Data to their employer while in the EU as part of the application process or otherwise;
- Participate in scientific or clinical research that involves receipt of Personal Data from the EU;
- Engage in certain kinds of targeted marketing in the EU, such as by attempting to recruit EU persons to become patients of a U.S. health care facility or service provider; or
- Employ certain vendors within the EU (i.e., "processors").

### **Controllers and Processors**

As mentioned above, the GDPR applies to persons or entities that are "controllers" or "processors" of Personal Data. A controller is an individual or legal entity that, acting alone or with others, determines the purposes and means of processing Personal Data. A processor, on the other hand, processes Personal Data on behalf of the controller, including activities such as data analytics, data storage, and data alteration. For example, if a U.S. health care institution targets EU individuals in a marketing campaign, and retains an email or marketing agency to assist in the campaign, the health care institution would be the controller and the email or marketing agency would be the processor with respect to any associated Personal Data. Or, if a U.S. hospital uses a call center to help monitor patients who had been treated in the United States after their return to Europe, the hospital would be the controller and the call center would be the processor of the personal data.

<sup>1</sup> These terms are defined below.

<sup>2</sup> Each EU member state will likely adopt its own rules with respect to GDPR compliance; thus businesses with significant contacts in the EU may need the assistance of local counsel in connection with each applicable EU member state. Currently, the U.K. has indicated it intends to follow the GDPR; however, post-Brexit, it is unclear whether the U.K. will implement its own separate set of rules.

### **Personal Data Protected by the GDPR**

In some respects, the GDPR is similar to the HIPAA Privacy and Security Rules that have applied to U.S. health care providers for over 15 years. Both regulatory regimes mandate that certain organizations ("covered entities" and "business associates" under HIPAA, "controllers" and "processors" under the GDPR) protect the privacy and security of certain categories of information. In contrast to HIPAA which applies to "protected health information" (PHI),<sup>3</sup> the GDPR covers all Personal Data about an identified or identifiable individual residing in the EU, even if temporarily. Accordingly, U.S. health care organizations subject to the GDPR will have to adjust their privacy and security policies to account for the broader definition of protected information under the new EU regulation.

Moreover, under the GDPR, certain kinds of Personal Data are subject to stricter privacy and security requirements. In addition to data about race, ethnicity, political opinions and religious beliefs, among other personal characteristics, this special category includes the following types of health-related information:

- "Data Concerning Health" – Personal Data related to the physical or mental health of an individual, including the provision of health care services, which reveals information about the individual's health status. This category of protected data is similar but not identical to "protected health information" under HIPAA.
- "Genetic Data" – Personal Data relating to the inherited or acquired genetic characteristics of an individual which give unique information about the physiology or health of that individual and which result, in particular, from an analysis of a biological sample from the individual.
- "Biometric Data" – Personal Data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of an individual, which allow or confirm the unique identification of that individual, such as facial images.

Under the GDPR, health, genetic, and biometric data generally can be processed only with the individual's express consent, or if processing is necessary in connection with an individual's medical diagnosis or treatment, for certain public health functions, for research, or for other limited purposes defined in the GDPR. The exceptions to the requirement of patient consent under the GDPR are different from and arguably more limited than those under HIPAA; for example, the exceptions do not encompass the broad categories of treatment, payment and operations.

### **What are the Major GDPR Requirements?**

Among other things, the GDPR requires a covered institution to:

- Appoint a person (called a "Data Protection Officer") to oversee protection of Personal Data;
- Provide notice regarding the Personal Data it collects, and how it uses such Personal Data;
- Record the uses and disclosures it makes of Personal Data;
- Obtain specific consent for collection of certain kinds of Personal Data;
- Allow individuals whose Personal Data was collected to object to such collection or processing, and ultimately honor an individual's "right to be forgotten," unless a legitimate basis exists to maintain the data;
- Ensure that all vendors and third parties to which it provides Personal Data have adequate privacy and security protections;
- Enter into contracts containing specific provisions when transferring Personal Data outside of the EU (including transferring within the institution); and
- Notify EU regulators, and potentially impacted data subjects, as soon as possible (where feasible, within 72 hours) after becoming aware of a data breach.

<sup>3</sup> For this purpose, health information means information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

***Building GDPR Policies on the Framework of HIPAA***

Many of the policies and operational steps to implement the GDPR are similar to HIPAA. For example, the requirement to appoint a Data Protection Officer to oversee the policy and data protection tracks closely to the obligations for a Privacy Officer. Similarly, the requirements to track the use and disclosure of Personal Data, to provide an accounting upon request, and enter into agreements to protect Personal Data with third parties that receive the data, are all similar to the requirements of HIPAA. For this reason, health care providers can build their GDPR policies on the framework of their HIPAA policies. At the same time, other elements of the GDPR are distinct from HIPAA and will require health care providers in the U.S. covered by the GDPR to adopt new privacy policies and procedures.

***Conclusion: Preparing for the GDPR***

U.S. health care organizations covered by the GDPR, directly or through the exchange of data with vendors, may be required to review and make appropriate modifications to a host of policies, including: (i) employment policies; (ii) data collection policies and procedures; (iii) policies for patient consent, especially when one or more of the special data categories are involved (see above); (iv) research protocols; and (v) procedures governing patient monitoring. Business Associate Agreements must also be modified to cover certain mandated GDPR clauses.

If you have any questions about this memorandum, or the steps necessary for GDPR compliance, contact Tracy E. Miller or Robert W. Patterson.

**Tracy E. Miller**  
(tmiller@bsk.com)

**Robert W. Patterson**  
(rpatterson@bsk.com)

## Employers May Be Liable for the Release of Employees' Personally Identifying Information in Data Breaches

It seems that reports of hackers breaching a business's security measures to obtain customer information appear on an almost weekly basis. Unfortunately, businesses need to worry not only about the unauthorized access of customer data by hackers, but also the unauthorized access of sensitive employee information as well.

The Pennsylvania Supreme Court recently held in *Dittman v. UPMC* that employers have a duty to use reasonable care to protect the unauthorized release of their employees' data, and that they could be liable to their employees for release of that data even where it was the result of a third-party's criminal activity. Several other cases have been brought around the country, including a 150,000 member class action brought by the National Treasury Employees' Union against the United States Office of Personnel Management, as a result of the hacking of employee data.

Employers in New York are prohibited from communicating an employee's personal identifying information ("PII") to the general public by Section 203-d of the New York Labor Law ("NYLL"). PII includes social security numbers, home addresses, telephone numbers, personal email addresses, internet screen names and passwords, a parent's surname before marriage, and drivers' license numbers.

In *Sackin v. Transperfect Global, Inc.*, Judge Schofield of the U.S. District Court for the Southern District of New York held that NYLL § 203-d gave the plaintiffs a private right of action against their employer for the unauthorized release of their PII due to a data breach. At least one Transperfect employee received a phishing email, purporting to be from the CEO, that was actually sent by hackers, and provided the hackers with the W-2 forms and payroll information of all current and former Transperfect employees. The plaintiffs alleged that Transperfect failed to train its employees on data security, to utilize firewalls, and to maintain retention and destruction protocols for PII. They also asserted that hackers could use the employees' PII to fraudulently obtain loans and credit cards, and to fraudulently file tax returns. After the breach, Transperfect offered the plaintiffs two years of free identity theft monitoring, but the plaintiffs purchased services to prevent identity theft instead.

The court found that the risks of identity theft set forth by the plaintiffs, as well as the costs incurred in purchasing identity theft protection services, gave the plaintiffs standing to sue their employer. Like the Pennsylvania Supreme Court in *Dittman*, it also acknowledged an employer's duty to reasonably protect its employees' PII. Ultimately, the court allowed the plaintiffs to proceed with their class-action against Transperfect under theories of negligence, negligence per se, breach of implied contract, and unjust enrichment, in addition to the statutory claim under NYLL § 203-d that was recognized by the court.

As this is an emerging area of the law, it is unclear whether an employer that took reasonable measures to avoid the breach of its data systems by hackers would be able to avoid liability. However, an employer will likely be in a better position to defend itself if it can show that it made reasonable efforts to secure its systems, updated its security measures periodically, and trained employees regularly regarding how to recognize phishing e-mails and other attempts to gain unauthorized access to confidential information.

Although most employers strive to protect their employees' PII, it is clear that in this day and age even the most secure systems are vulnerable to attack by sophisticated hackers. In the event that your business's data systems are breached and employee, customer, client or other third-party data is released, our firm can assist you in responding and complying with all applicable reporting requirements.

If you have any questions about this Information Memo, please contact Nicholas P. Jacobson.

**Nicholas P. Jacobson**  
([njacobson@bsk.com](mailto:njacobson@bsk.com))

Copyright License and Release  
Law360® Expert Analysis Submission

**Title/Description of Work:** "New York Cybersecurity Regulations Reach Beyond Financial Sector to Health Care Plans and Providers"

**Author:** Tracy E. Miller

**Date:** March 20, 2017

**Copyright Holder (organization or individual):** Tracy E. Miller

**Licensor (organization or individual):** Tracy E. Miller

**Licensor Address:** Bond, Schoeneck & King, PLLC, 600 Third Ave., 22<sup>nd</sup> Floor, NY NY 10016

**Phone:** 646-253-2308

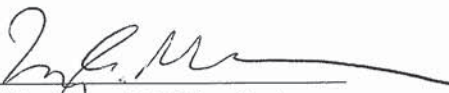
**Email:** tmiller@bsk.com

This Agreement may be signed electronically by Licensor, subject to Licensor inserting the following text directly above his/her signature in the area designated below: *"I agree, and it is my intent, to sign this Agreement and affirmation by entering my name, preceded and followed by the forward slash (/) symbol (e.g., "/John Doe/") and by electronically submitting this Agreement to PMI. I understand that my signing and submitting this Agreement in this fashion is the legal equivalent of having placed my handwritten signature on the submitted Agreement and this affirmation. I understand and agree that by electronically signing and submitting this Agreement in this fashion I am affirming to the truth of the information contained therein."*

The undersigned has read and agrees to be bound by the terms and conditions set forth in the Agreement appended hereto and knows and understands the full content thereof.

LICENSOR

[INSERT AFFIRMATION FROM ABOVE IF APPLICABLE]

By:   
Name/Title: Tracy E. Miller, Partner

**Copyright License and Release**  
**Law360® Expert Analysis Submission**

This agreement ("**Agreement**") is entered into by Portfolio Media, Inc. (collectively with its subsidiaries and affiliates, including any future affiliates, "**PMI**") and the Licensor specified above (the "**Licensor**") as of the date specified above.

For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Licensor, on behalf of itself and as applicable, on behalf of Author (if specified above), agrees as follows:

1. GRANT OF LICENSE

- 1.1. "Licensed Materials" means the materials specified above, including all text, artwork, images, photographs, languages, editions, issues, versions and updates published or otherwise made commercially available during the term of this Agreement.
- 1.2. Licensor hereby grants to PMI an irrevocable, unqualified, transferable, fully-paid-up, royalty-free, worldwide license (with the right to license and sublicense at multiple levels) and release (the "**License**") to use and authorize use of the Licensed Materials including the exercise of all rights of whatever kind or nature now or hereafter protected by the Copyright Laws of the United States of America and all foreign countries (including without limitation, the right to use, exploit, copy, publish online on PMI's website (the "**Site**"), a website of an affiliate, or otherwise, reformat, adapt, translate, display, excerpt in whole or in part, and distribute in any form, medium or technology, for any purpose on or in connection with the Site, PMI's business, or the promotion thereof) in and to the Licensed Material. Without limiting the generality of the foregoing, the Licensor further grants to PMI the rights to edit, publish, reproduce, reprint, distribute, sell, and otherwise make use of the work, and authorizes PMI to use the Author's name, likeness, photograph, and biographical data in connection with PMI's use and promotion of the work on the Site or elsewhere (including without limitation the websites of affiliates of PMI). Licensor hereby agrees and acknowledges that for a period of **three (3) months** from the date of this Agreement (the "**Exclusivity Period**"), the License shall be an exclusive license and, thereafter, the License shall be a perpetual, non-exclusive license; provided that nothing herein shall restrict Licensor's ability during the Exclusivity Period to (x) display the Licensed Material on Licensor's own website or blog, (y) include the Licensed Material in Licensor's newsletter or similar publication produced by Licensor, and (z) utilize the Licensed Material in Licensor's internal training materials so long as, in each case, the Licensed Material is not thereby provided to any other media organization; provided that the Licensed Material may be submitted for publication to content or news aggregators (including, without limitation, Lexology or Mondaq) so long as such content or news aggregators are not competitive with PMI or its business.
2. It is understood that, other than the good and valuable consideration received for this license and release, neither the Licensor nor the Author has received, nor will either of them receive, any royalty or other monetary compensation from PMI for the rights granted hereunder and the subsequent use of the work by PMI and it is further understood and acknowledged that neither Licensor nor Author is entitled to any such royalty or monetary compensation.
3. Licensor understands and acknowledges that the Licensed Material may be displayed or posted on the Site in such a way as to permit visitors to the Site, who may be unaffiliated with the Site or PMI, to post or publish comments ("**Comments**") about the Licensed Material. Licensor understands and agrees that with respect to any Comments, the Site acts merely as a passive conduit for any and all communication and/or distribution of information, and PMI does not control the Comments. PMI cannot and will not evaluate, and PMI is not responsible for the accuracy, reliability, completeness, veracity or suitability of, any Comments or for verifying the identity of any party posting a Comment. While PMI will endeavor to monitor Comments on the Site and



flag and/or remove Comments which are found to be unsuitable for the Site (as determined by PMI in its sole and absolute discretion) PMI shall be under no obligation to do so.

4. The Licensor represents and warrants to PMI, on behalf of itself and, if Licensor is not Author, on behalf of Author, that the Licensed Materials are the Author's own original work; that the Author is the sole owner of the work and all of the rights herein granted (including, without limitation, the rights granted to PMI herein to use any artwork, images or photographs included in the Licensed Materials); that the Licensor has the full right, power and authority to make this license and release on behalf of itself, on behalf of the Author and, as applicable, on behalf of Author's employer; that the Licensed Materials do not violate any copyright, proprietary or personal rights of others; that the work is factually accurate and contains no matter libelous or otherwise unlawful; that neither Licensor, Author or Author's employer has previously in any manner disposed of any of the rights herein granted to PMI nor previously granted any rights adverse thereto or inconsistent therewith; and that there are no rights outstanding which would diminish, encumber or impair the full enjoyment or exercise of the rights herein granted to PMI.
5. The Licensor agrees to release, indemnify and hold harmless PMI and its officers, directors, members, employees, and agents, from and against any and all claims, actions, losses, demands, costs, attorneys' fees, and all other expenses relating or incidental to, or arising directly or indirectly from, the inaccuracy or breach of any of the aforementioned warranties and representations, including, without limitation, any and all claims by Author or Author's employer against PMI.
6. Licensor further declares, represents and warrants that no promise, inducement or agreement not herein expressed has been made to Licensor.
7. This Agreement contains the entire agreement between Licensor and PMI with respect to its subject matter and supersedes any prior or contemporaneous agreements, whether written or oral. This Agreement shall be construed and interpreted in accordance with the laws of the State of New York without regard to its conflicts of laws principles. This Agreement may only be modified in writing signed by these parties.

