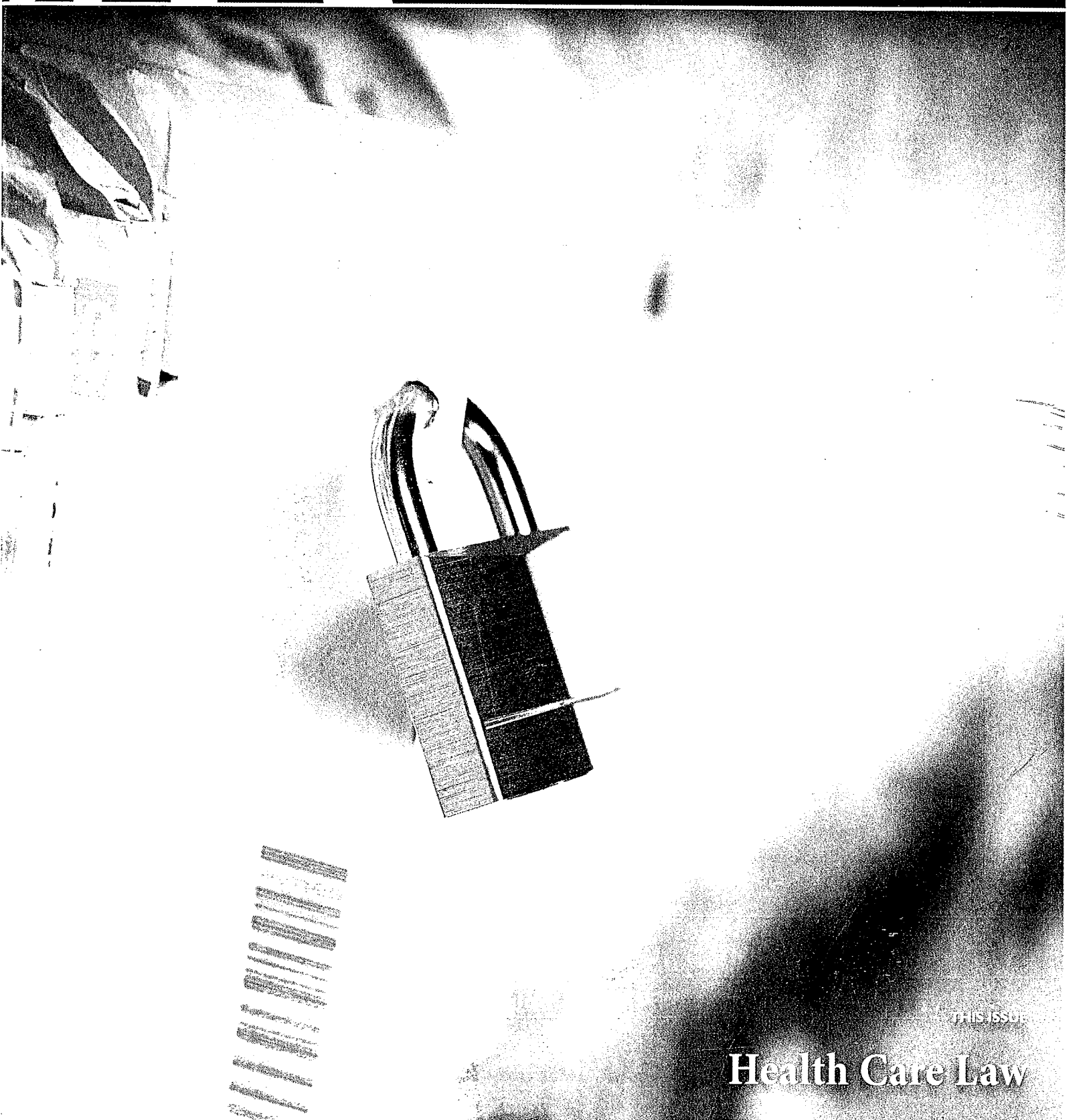
BAR JOURNAL

OF THE CLEVELAND METROPOLITAN BAR ASSOCIATION
VOL. 6 NO. 8 | MARCH 2014



IN THIS ISSUE:

Health Care Law

Common Myths of HIPAA's "Final Rule" — What Every Practitioner Should Know

BY MARILENA DISILVIO & DAVID A. VALENT

This past year the Federal Government published changes to HIPAA that required health care providers (aka "covered entities") to update their practices relative to the protection of patient health information. These changes are codified in the section of Federal Code often referred to as HIPAA's "Final Rule." 78 FR 5565, 45 CFR 160; 45 CFR 164 (Jan. 25, 2013). While the changes became effective March 26, 2013, covered entities had until September 23, 2013 to implement the changes before penalties would be enforced.

With the implementation of the Final Rule changes, vendors and health care lawyers alike have been scrambling to publish information to explain, in practical terms, what these changes will mean to those in the health care industry. Unfortunately, through this rush of information, many hyperboles have been disseminated, leaving health care providers with confusion as to what is actually required by the new rules.

Amongst the confusion, some health care providers have taken the "not me approach" and concluded that because the law is confusing and/or uncertain, it cannot possibly be enforced and/or require "me" to change the way I am doing business. On the other hand, some providers have gone to the other extreme, and have changed everything about the way they store, share and communicate protected health information. Such drastic changes have, in some cases, resulted in the unnecessary expenditure of thousands of dollars, and the unnecessary impairment to the flow of communication between care providers.

This article is intended to cure some common myths, and provide a better understanding of the Final Rule, so that you can more effectively triage and answer your clients' privacy related questions.

All Changes Outlined in the Final Rule are Mandatory, and Must be Implemented.

Myth. The Final Rule identifies those aspects of privacy management that are "required" to be implemented, as well as those that are merely "addressable." That said, the addressable provisions cannot be ignored. In the event of a government audit and/or investigation, a covered entity will need to establish that it did indeed "address" all the aspects of the Final Rule. All covered entities must address all aspects of the Final Rule, and come to a reasonable conclusion as to which measures to implement.

Providers with "Good" Privacy Practices Need Not Make Any Changes.

Myth. The Final Rule provides that all covered entities must undertake what is known as a "risk analysis." The risk analysis is at the core of the new rule changes. Although a practice may already have a number of security measures in place, those measures need to be reviewed, and improved, where appropriate. The Final Rule requires that each covered entity assess its administrative safeguards, technical safeguards and physical safeguards relative to protecting patient information.

There is no law requiring that providers use the assistance of an attorney with conducting a risk analysis. That said, involving an attorney can help ensure the confidentiality and propriety of the process.

Providers Cannot Send Protected Health Information Electronically, Unless It Is Encrypted.

Myth. Many providers believe that all emails containing protected health information must be encrypted. This is not necessarily true. The Final Rule provides that transmitting electronic health information is an addressable matter. This means that each practice must address whether it is practical and/or necessary to send unencrypted emails, given

the nature of their practice and potential risk to privacy. In the event that a practice decides to send unencrypted emails, the practice should nevertheless consider other methods or means to improve the security of sending such emails. For example, limiting the scope of the information sent, sending emails only when no other reasonable alternative exits, and sending only to those individuals whose email addresses have previously been confirmed, are all ways to limit the risk of a breach.

Moreover, faxing health information remains an acceptable practice for sending health information under HIPAA's Final Rule.

Small Practices Are Not Subject to the Same Rules as Large Practices, or Hospitals.

Myth. All covered entities are subject to the Final Rule. Of course, the size and nature of a practice may dictate the manner in which the "addressable" provisions of the Final Rule are implemented. For example, it may not be practical and/or necessary for smaller practices to implement certain changes — such as using encryption to send emails.

Only Those Providers Who Willfully Breach Privacy Rights Are Subject to Fines.

Myth. The Office of Civil Rights prosecutes civil and criminal penalties for violations of patient privacy rights, even if a provider does not have the intent to commit a breach. In civil cases, the law indeed provides for mitigating and aggravating factors that can affect the amount of a monetary penalty — such as the level of culpable mindset. Still, even providers who act without knowledge as to a HIPAA violation can be subject to a penalty of up to $1.5 million per year, for all violations related to a single provision of HIPAA.

Law Firms, Working with Health Care Providers, Are Not Subject to HIPAA.

Myth. Pursuant to the Final Rule, business associates (such as law firms) must now comply with many parts of HIPAA, including the Security Rule.

Business Associates are outside persons or entities that perform services for the health care provider. Examples of business associates include law firms, billing services, and document storage companies. Health care providers must have business associate agreements with their business associates, containing specific language, as required by the Final Rule. The business associate agreements, as well as the Final Rule, impose obligations on business associates.

The Government can directly impose penalties on business associates, and their subcontractors, if compliance does not occur.

All Unintended Disclosures of Health Information Constitute a Breach, and Notification Is Required.

Myth. A "breach" only occurs when the privacy or security of patient information is compromised, as a result of someone acquiring, accessing, using or disclosing information in violation of the Privacy Rule, without any exception applying.

One exception would be the inadvertent disclosure of "secured" information. For example, if information is properly secured and/or encrypted, pursuant to the definitions outlined by HIPAA, then sending such information to the wrong person does not necessarily constitute a breach. This is because the information cannot be accessed by individuals not intended (and/or without appropriate passwords) to access same. This is one reason why encryption is encouraged by the Final Rule, as it eliminates breaches from occuring in certain circumstances.

Another exception would include the inadvertent disclosure of protected health information among workers and/or business associates of the same health care entity. For example, if a provider inadvertently discloses protected health information to a business associate, relative to a patient record in which that business associate did not otherwise have access, such disclosure is not necessarily a breach.

Now, even if a recognized exception does not apply, and a breach does occur, there are still instances wherein notification is not required. If a health care provider performs an appropriate written assessment and confirms there is a low probability that the information has been compromised, then, it may be reasonable for that provider to conclude that notification is not required. At a minimum, the assessment should consider:

- The nature and extent of the patient information involved, including the types of identifiers contained within the information;
- The unauthorized person who used the patient information or to whom the disclosure was made;
- Whether the patient information was actually acquired or viewed; and
- The extent to which the risk to the patient has been mitigated.

Following a written assessment of the above factors, a health care provider may reasonably determine whether it is necessary to notify anyone, including the affected individual, the Department of Health and Human Services, or the media.

* * *

Above are just a few of the common myths that have evolved since the implementation of HIPAA's Final Rule in 2013. It is important when discussing these issues with clients that the prepared lawyer understands there is an excess of misinformation circulating on this topic. It is wise to address the Final Rule itself when advising a client on these matters. The HIPAA Final Rule can be accessed at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html. For further information and/or consultation regarding the protection of patient privacy rights please contact the authors.

Marilena DiSilvio is the Chair of Reminger's Health Care Law Practice Group. She devotes the majority of her professional time to the representation of health care providers. She has been named many times a Best Lawyer in America, and as an Ohio Super Lawyer. She has been a CMBA member since 1995. She can be reached at mdisilvio@reminger.com or (216) 687-1311.

David A. Valent is a leading member of Reminger's Health Care Law Practice Group. He has also twice been recognized as an Ohio Rising Star. He has been a CMBA member since 2008. He can be reached at dvalent@reminger.com or (216) 687-1311.