2013 URMIA Journal Reprint

Does Your Insurance Policy Protect Against Liability Under the New HIPAA Regulations?

Jerold Oshinsky
Kasowitz Benson

Linda D. Kornfeld
Kasowitz Benson

Kirsten C. Jackson
Kasowitz Benson

University Risk Management and Insurance Association

URMIA

In order to lead a country or a company, you've got to get everybody on the same page and you've got to be able to have a vision of where you're going. America can't have a vision of health care for everybody, green economy, regulations - can't have a bunch of piece-meal activities. It's got to have a vision.

—Jack Welch (1935–),

American Business Executive and Past CEO of General Electric

Does Your Insurance Policy Protect Against Liability Under the New HIPAA Regulations?

| *Jerold Oshinsky, Linda D. Kornfeld, and Kirsten C. Jackson, Kasowitz Benson*

Abstract: On March 26, 2013, the Omnibus Rule went into effect, including important changes to the Health Insurance Portability and Accountability Act's (HIPAA) Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act (GINA). These changes may result in increased liability for university hospitals, also impacting other university-owned health care providers and their business partners. This article highlights these changes and offers ways for colleges and universities to ensure they are meeting their HIPAA requirements and the new requirements under the Omnibus Rule.

Introduction

On January 17, 2013, the US Department of Health and Human Services announced important modifications to the Health Insurance Portability and Accountability Act's (HIPAA) Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act (GINA).[1] These changes are known as the Omnibus Rule. The Omnibus Rule went into effect on March 26, 2013, and covered entities must comply with the requirements of the Omnibus Rule by September 23, 2013.[2] These new requirements may result in increased potential liability by university hospitals and other university-owned health care providers, not only for their own alleged HIPAA violations but also for violations of HIPAA by business partners. This article highlights the key changes to HIPAA that may affect universities, as well as explains the ways in which universities may protect against possible increased risk exposure.

The Omnibus Rule added a number of important new regulations as to how health care providers must treat protected health information, which go above and beyond pre-existing HIPAA regulations.

Overview of the New HIPAA Omnibus Rule

Under the new HIPAA Omnibus Rule, breach has been more broadly defined, penalties have been substantially increased, and covered entities (including university hospitals) may now be liable for violations by business associates and subcontractors. These key changes, which could increase universities' potential liability under HIPAA, are as follows:

New Regulations on the Treatment of Protected Health Information

The Omnibus Rule added a number of important new regulations as to how health care providers must treat protected health information. The new regulations limit the use and disclosure of protected health information for marketing and fundraising purposes.[3] They also prohibit the sale of protected health information without individual authorization.[4] These regulations go above and beyond pre-existing HIPAA regulations, under which health care providers were already required to comply with strict administrative safeguards and notification and documentation requirements deemed necessary to ensure the safety of protected health information.

One of the most significant developments in the Omnibus Rule is its change in the definition of what constitutes a breach. Previously, a breach required a finding that the access, use or disclosure of personal health information posed "a significant risk of financial, reputational, or other harm to an individual."[5] This harm threshold had to be met before health care providers were required to notify patients of the breach.

The Omnibus Rule replaces the "harm threshold" with a new standard.[6] Under the new regulations, a breach is presumed whenever protected health information is

acquired, accessed, used, or disclosed in a way that violates HIPAA's stringent standards. Patients must be notified unless a risk assessment demonstrates that there is a "low probability that the protected health information has been compromised."[7] This risk assessment must take into account four factors: "(1) to whom the information was impermissibly disclosed; (2) whether the information was actually accessed or viewed; (3) the potential ability of the recipient to identify the subjects of the data; and (4) in cases where the recipient is the disclosing covered entity's business associate or is another covered entity, whether the recipient took appropriate mitigating action."[8]

Any failure of university hospitals—or, as we will see, their business associates, subcontractors, and other agents—to follow the new, stricter rules regarding the treatment of protected health information may expose them to liability for HIPAA violations. Under the new Omnibus Rule these penalties have increased.

Penalties for HIPAA Violations Have Increased

Under the new Omnibus Rule, there are now four categories of violations that reflect increasing levels of culpability and four corresponding tiers of penalty amounts that increased the minimum penalty amount for each violation.[9] The maximum penalty is now $1.5 million annually for all violations of an identical provision.[10] However, as the US Department of Human Health Services warns, "a covered entity or business associate may be liable for multiple violations of multiple requirements, and a violation of each requirement may be counted separately. As such, one covered entity or business associate may be subject to multiple violations of up to a $1.5 million cap for each violation, which would result in a total penalty above $1.5 million."[11]

At the same time that the penalties for HIPAA violations have expanded, affirmative defenses for these violations have narrowed. The Omnibus Rule removes the previous affirmative defense to the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation.[12] Moreover, previously there were no penalties for violations that were corrected in a timely manner unless the violation was due to willful neglect. However, under the new Omnibus Rule, penalties may now be imposed even for violations that are timely corrected.[13]

Due to the increases in fines and penalties, now more than ever, violations of HIPAA's regulations could result in potential liability for university hospitals and other university-owned health care providers.

Business Associates and Subcontractors Are Directly Liable for HIPAA Violations

The new Omnibus Rule not only affects health care providers like university hospitals, but makes business associates of these entities directly liable for compliance with many of the HIPAA Privacy and Security Rules' requirements. The Omnibus Rule defines "business associate" as a person or entity "'who creates, receives, *maintains*, or transmits' (emphasis added) protected health information on behalf of a covered entity."[14] Moreover, now "subcontractors"—persons "to whom a business associate delegates a function, activity, or service"—are specifically included in the new definition of "business associate."[15] The rules are not simply limited to direct subcontractors but also apply to "downstream entities."[16]

Previously, business associates and their subcontractors could only be held liable for breach of their contracts with health care providers. Under the new Omnibus Rule, however, business associates and subcontractors are directly liable for HIPAA violations.[17] It is necessary for business associates and subcontractors to follow all rules regarding the use and disclosure of protected health information due to their potential liability. Moreover, it is necessary for university hospitals to closely monitor their business partners, as under the new Omnibus Rule hospitals face potential risk of vicarious liability.

Health Providers Liable for Violations by Business Associates and Subcontractors

The new Omnibus Rule could increase the likelihood that university hospitals and other health care providers will face liability for conduct by business partners. This is significant, as by some estimates these business partners, rather than the health care providers themselves, are responsible for more than 60 percent of HIPAA violations.[18]

Previously, health care providers were excepted from liability for the acts of agents where the agent was a business associate, the relevant contract requirements had been met, the covered entity did not know of a pattern or

practice of the business associate in violation of the contract, and the covered entity did not fail to act as required by the Privacy or Security Rule with respect to such violations.[19] The new Omnibus Rule does away with this exception.[20] Moreover, the Omnibus Rule adds a parallel provision that creates a civil money penalty liability against a business associate for the acts of its agent.[21] Under the new rule, it does not matter whether the health provider or business associate has a HIPAA-compliant business agreement in place.[22]

The Omnibus Rule applies the federal common law of agency.[23] Whether a business associate is an agent is fact-specific and turns largely on the right or authority of the health provider to control the business associate's conduct in the course of performing a service on its behalf.[24] The right or authority to control is likewise the essential factor in determining whether an agency relationship exists between a business associate and its business subcontractor.[25]

The US Department of Health and Human Services has given some helpful examples regarding how agency applies:

> A business associate generally would not be an agent if it enters into a business associate agreement with a covered entity that sets terms and conditions that create contractual obligations between the two parties. Specifically, if the only avenue of control is for a covered entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a business associate is not acting as an agent. In contrast, a business associate generally would be an agent if it enters into a business associate agreement with a covered entity that granted the covered entity the authority to direct the performance of the service provided by its business associate after the relationship was established. For example, if the terms of a business associate agreement between a covered entity and its business associate stated that "a business associate must make available protected health information in accordance with § 164.524 based on the instructions to be provided by or under the direction of a covered entity," then this would create an agency relationship between the covered entity and business associate for this activity because the covered entity has a right to give interim instructions and direction during the course of the relationship. An agency relationship also could exist between a covered entity and its business associate if a covered entity contracts out or delegates a particular obligation under the HIPAA Rules to its business associate.[26]

The right or authority to control is the essential factor in determining whether an agency relationship exists between a business associate and its business subcontractor.

The US Department of Health and Human Services has warned that a "business associate can be an agent of a covered entity: (1) Despite the fact that a covered entity does not retain the right or authority to control every aspect of its business associate's activities; (2) even if a covered entity does not exercise the right of control but evidence exists that it holds the authority to exercise that right; and (3) even if a covered entity and its business associate are separated by physical distance (e.g., if a covered entity and business associate are located in different countries)."[27] The new Omnibus Rule could potentially increase the possibility of liability by university hospitals and other university-owned health care providers for the actions of third parties.

Insurance Coverage for HIPAA Violations

Given the addition of new regulations under HIPAA, an increase in fines and penalties for HIPAA violations, and the possibility of broader liability for the acts of business partners under the new Omnibus Rule, it is essential that university hospitals and other university-owned health care providers protect themselves against potential risk exposure. Federal enforcement of HIPAA claims against health care providers is on the rise. Insurance is an important means of protecting universities from the costs of defense against these claims, as well as from fines and penalties if liability is found.

Traditional D&O and E&O policies may provide coverage for HIPAA violations unless explicitly excluded. For example, even under policies that do not have express penalty coverage, HIPAA violations still may be covered.[28] Moreover, it may be possible to obtain coverage for business associates and subcontractors as "independent contractors" insured under a traditional policy. At least one court has rejected an insurer's attempt to narrowly construe independent contractor language in a healthcare D&O policy.[29] However, recently many insurance companies have developed health care policies that provide coverage specifically for HIPAA investigations. These policies cover defense costs and penalties associated with HIPAA violations.

Time is of the essence. The new HIPAA Omnibus Rule went into effect on March 26, 2013, and university hospitals will only have until September 23, 2013, to comply with the new requirements. Now is the time to re-examine your insurance policy to ensure that you are protected against potential liability under the new HIPAA Omnibus Rule.

Broad Definition of Loss

Given what is at stake, universities should consult with experienced insurance counsel to ensure their policies include coverage for violations of HIPAA. Certain insurers provide coverage specifically for losses associated with HIPAA violations. For example:

> **"Loss"** means damages, judgments (including pre/post-judgment interest on a covered judgment), settlements, and Defense Costs; however, Loss shall not include:
>
> 1. civil or criminal fines or penalties imposed by law, **except**:
> 2. HIPAA Penalties, subject to the HIPAA Penalties Sublimit of Liability set forth under Clause 6 "LIMIT OF LIABILITY (FOR ALL LOSS – INCLUDING DEFENSE COSTS)" of this policy.

In this particular example, "wrongful act" was defined as "the failure to comply with the privacy provisions of HIPAA." Likewise, "HIPAA penalties" included "civil money penalties imposed upon an Insured for violation of the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 and any amendments thereto."[30]

In another example, an insurance policy provided that:

> HEALTH INFORMATION PRIVACY AND NOTIFICATION COSTS
>
> Subject to the Information Privacy aggregate limit of liability stated on the certificate of insurance, we will:
>
> 1. Pay "HIPAA" fines and penalties pursuant to the Health Insurance Portability and Accounting Act "HIPAA", which you become legally obligated to pay arising from a "HIPAA" proceeding with respect to the management and transmission of confidential health information; and
> 2. Reimburse you for notification costs related to the disclosure of confidential personal information provided that you obtain our prior approval before incurring such costs.
> 3. Pay claim expenses related to 1. and 2. above.[31]

Unlike the first policy, this policy provides coverage for expenses associated with notifying patients of a breach that compromised their protected health information. Give that the standard for when breach notification is mandatory has been lowered, *see supra*, and given that the US Department of Health and Human Services has estimated that the costs of notification may run into the millions of dollars per year, this coverage may be desirable.

In sum, given the possible risks facing university hospitals following passage of the Omnibus Rule, broad coverage for losses stemming from HIPAA violations is essential.

Broad Investigations Coverage

Universities should also ensure that their policies contain broad investigations coverage, including coverage for loss arising from investigations brought by the government alleging HIPAA violations. For example, certain policies provide coverage explicitly for HIPAA investigations:

"HIPAA Proceeding" means an administrative proceeding, including a complaint, investigation or hearing instituted against you by the Department of Health and Human Services or its designee alleging a violation of responsibilities or duties imposed upon you under the Health Insurance Portability and Accountability Act ("HIPAA"), or any rules or regulations promulgated thereunder, with respect to the management of confidential health information.[32]

In this particular policy, the insuring agreement broadly provided express coverage for all "claims expenses" related to any "HIPAA Proceeding." Because not only the fines associated with HIPAA violations but defending against the investigations themselves can be quite costly, investigations coverage is necessary.

High/No HIPAA Penalties Sublimit

Moreover, universities should ensure their policies contain sublimits of coverage for HIPAA liabilities that meet their needs. In the above example, the policy contained a "HIPAA Penalties Sublimit of Liability:"

HIPAA PENALTIES SUBLIMIT OF LIABILITY:
The maximum limit of the Insurer's liability for all HIPAA Penalties, in the aggregate, shall be $ ___ (the "HIPAA Penalties Sublimit of Liability"). The HIPAA Penalties Sublimit of Liability shall be part of, and not in addition to, the Aggregate Limit of Liability set forth in Item 3(b) of the Declarations, and shall in no way serve to increase the Insurer's Aggregate Limit of Liability as stated therein.[33]

Because each HIPAA violation—whether by the university hospital or its business partners— could potentially result in up to $1.5 million in liability, universities must ensure this limit is appropriate to their needs. If possible, universities should negotiate with their insurer and obtain policies which offer full policy limits for fines, penalties and defense costs for HIPAA violations.

Given potential liability created by business associates' and subcontractors' activities under the new Omnibus Rule, universities should make sure that their policies cover the exposures of others.

Additional Insured Coverage

Given potential liability created by business associates' and subcontractors' activities under the new Omnibus Rule, universities should make sure that their policies cover the exposures of others. Where possible, university hospitals should add business associates and subcontractors to their list of additional insureds. Moreover, university hospitals should enter into agreements with their business associates and subcontractors whereby the latter would be responsible for obtaining additional insured coverage for the hospital under their own policies.

Cyber Liability Coverage

In certain circumstances, you may also want to consider purchasing a cyber liability policy that insures against liability for data security breaches, including protected health information under HIPAA. For example, certain insurance policies promise to reimburse insureds for:

"Security event costs" means (CYBER LIABILITY):
All reasonable and necessary fees, costs, and outside expenses you incur with our prior written consent in connection with a security breach, privacy breach or breach of privacy regulations, as described below:

1. Notification costs and related expenses that you incur to comply with requirements of governmental statutes, rules or regulations, or which you incur as a result of a judgment, settlement, consent decree, or other legal obligation, including the services of an outside legal firm to determine the applicability of and actions necessary to comply with governmental statutes, rules or regulations;
2. Computer forensic costs of outside experts retained to determine the scope, cause, or ex-

tent of any theft or unauthorized disclosure of information, but such expenses will not include your compensation, fees, benefits, or expenses of those of any of your employees;

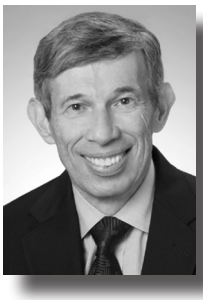
3. Credit protection services for the affected individual.[34]

However, it is worth noting that traditional insurance carriers may be reluctant to provide such broad insurance coverage for university hospitals, as colleges and health care organizations present unique risks due the inherently sensitive nature of student and patient records. University hospitals may need to consider not only traditional insurance carriers but also cyber-specific insurers in order to find the best available coverage.

Conclusion

If universities experience losses associated with HIPAA violations, they should act quickly to protect their rights. Insurance policies have strict deadlines in which to file notice of a claim, after which time the insurer will argue that coverage is lost. Moreover, at some point during the claims process, universities may need to litigate or arbitrate with an insurer. Universities should secure experienced insurance coverage counsel to ensure that they receive all the coverage to which they may be entitled.

About the Authors



Jerold Oshinsky is a litigator who represents policyholders in insurance coverage matters in federal and state courts throughout the country. Fortune 500 companies and other clients nationwide seek his advice on insurance coverage matters. Mr. Oshinsky is the only lawyer nationwide to be accorded "Star" ranking by Chambers USA in its national insurance category, achieving that recognition both in 2011 and 2012. Mr. Oshinsky litigates some of the most significant, complex insurance coverage issues in the country and also advises clients about how to maximize their insurance assets. He has worked with a variety of organizations, including chemical, pharmaceutical, financial, food, education, and health enterprises.

In addition to recognizing Mr. Oshinsky as "the foremost practitioner at the policyholder Bar" in 2012, Chambers USA also included him in its top tier "Band 1" ranking in California. In 2011, Legal 500 recognized Mr. Oshinsky as one of 13 "Leading Lawyers" nationally in its "Insurance: Advice to Policyholders" category. He was one of Law360's "10 Most Admired Attorneys" in 2010 and is regularly cited in Best Lawyers, Super Lawyers, and the Lawdragon 500 Leading Lawyers in America.

Mr. Oshinsky also maintains a pro bono practice. He has been lead counsel in numerous pro bono immigration appeals. Mr. Oshinsky frequently lectures and publishes on a wide variety of insurance law topics and serves as an expert witness in insurance coverage litigation matters.

Linda D. Kornfeld is a litigator who represents corporate and individual policyholders in high-stakes insurance coverage litigation. Ms. Kornfeld has substantial trial experience, and over the course of her career, she has assisted clients in obtaining hundreds of millions of dollars in insurance recoveries. She has helped clients ranging from universities, telecommunications companies, and real estate developers to manufacturers and non-profit organizations recover insurance assets both through negotiations and trial. She also provides strategic counseling to senior executives and in-house counsel on how to mitigate risk and maximize their insurance recoveries.

Ms. Kornfeld has been repeatedly cited as one of the top women lawyers in California by legal publications and directories, including Chambers USA. She also is listed as one of Lawdragon's top 500 "leading lawyers" in America, named by the *Daily Journal* as one of California's top women lawyers, by Benchmark Litigation as a "Litigation Star," and a Benchmark Top 250 Women in Litigation. Ms. Kornfeld is a frequently requested speaker, media resource, and author on complex litigation and insurance recovery issues. She is an advisory board member for the *Insurance Coverage Law Bulletin* and recently co-authored the treatise, *A Policyholder's Primer on Insurance*, published by the Association of Corporate Counsel. She is a member of the firm's Insurance Litigation and Counseling Practice.

Ms. Kornfeld also is involved in women's leadership issues and actively promotes the advancement of women into leadership positions in the legal and other professions. A frequent speaker and writer on women's issues, she serves as a West Coast leader of the Women's Leadership & Mentoring Alliance.

Kirsten Jackson is an associate at Kasowitz, Benson, Torres & Friedman LLP and has experience in a wide variety of insurance coverage disputes. Ms. Jackson is a member of several professional associations, including the American Bar Association, of which she is the co-chair of the Insurance Coverage Litigation Committee's Social Media Subcommittee.

Ms. Jackson maintains an active pro bono practice, having represented several pro bono clients on appeal before the US Court of Appeals for the Ninth Circuit.

Ms. Jackson graduated from Stanford University in 2006, receiving a Bachelor of Arts in history and psychology. She received a full scholarship to Columbia University School of Law, where she was a Hamilton Fellow and Stone Scholar, and earned a Juris Doctor in 2009. While attending Columbia, Ms. Jackson served as a senior editor on the *Columbia Law Review*.

Endnotes

1 Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (January 25, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

2 Ibid.

3 Ibid.

4 Ibid.

5 Ibid., 5639.

6 Ibid., 5566.

7 Ibid., 5641.

8 Ibid.

9 Ibid., 5577.

10 Ibid.

11 Ibid., 5584.

12 Ibid., 5585.

13 Ibid., 5586.

14 Ibid., 5572.

15 Ibid., 5573.

16 Ibid.

17 Ibid., 5566.

18 HIPAA Compliance, http://www.hipaa.co/hipaa-compliance.

19 78 Fed. Reg. 5566, 5580.

20 Ibid.

21 Ibid.

22 Ibid.

23 Ibid.

24 Ibid., 5581.

25 Ibid.

26 Ibid.

27 Ibid., 5582.

28 For example, on January 6, 2012, San Francisco Superior Court Judge Howard Kahn ruled that under the California Invasion of Privacy Act, statutory damages were not "fines, . . . sanctions or penalties" but rather covered "damages," holding they represent a form of "statutory liquidated damages" set by the legislature in circumstances where the actual damages from a breach event are difficult to measure. *Visa Inc. v. Certain Underwriters at Lloyd's, London*, Case No. CGC-11-509839 (January 6, 2012).

29 On January 15, 2013, Santa Barbara Superior Court Judge Thomas Anderle rejected an insurer's argument that doctors could not be "independent contractors" because they did not under the "exclusive direction" of the hospital. The Court held that the definition of "independent contractor" as being under the "exclusive direction" of the hospital was ambiguous and denied the insurer's motion for summary judgment. *Cottage Health System v. Travelers Cas. & Sur. Co.*, Case No. 13821220 (Jan. 15, 2013). The authors of this article represented the insured hospital in this case.

30 Chartis Insurance, "9/99 Amendatory Endorsement," http://www.chartisinsurance.com/ncglobalweb/internet/US/en/files/AIG%20Executive%20Liability-%209.99%20Amendatory%20Endorsement%205-28-08_tcm295-92662.pdf.

31 CNA Insurance, "Information Privacy Coverage Endorsement: 'HIPAA' Fines and Penalties and Notification Costs," http://www.nso.com/policyforms/m3/GSL-15563.pdf.

32 Ibid.

33 Chartis Insurance, "9/99 Amendatory Endorsement."

34 Philadelphia Insurance Companies, "Cyber Security Liability Coverage Form," May 2010, https://www.phly.com/Files/CyberSecurityLiabilityPolicy_Admitted31-932.pdf.

The *URMIA Journal* is published annually by the University Risk Management and Insurance Association (URMIA), PO Box 1027, Bloomington, IN 47402-1027. URMIA is an incorporated non-profit professional organization.

The 2013 *URMIA Journal* was edited and designed by Christie Wahlert, URMIA, Bloomington, Indiana; and the *URMIA Journal* was printed at Indiana University Printing Services, Bloomington, Indiana.

There is no charge to members for this publication. It is a privilege of membership, or it may be distributed free of charge to other interested parties. Membership and subscription inquiries should be directed to the National Office at the address above.

© LEGAL NOTICE AND COPYRIGHT: The material herein is copyright July 2013 URMIA; all rights reserved. Except as otherwise provided, URMIA grants permission for material in this publication to be copied for use by non-profit educational institutions for scholarly or instructional purposes only, provided that (1) copies are distributed at or below cost, (2) the author and URMIA are identified, (3) all text must be copied without modification and all pages must be included; and (4) proper notice of the copyright appears on each copy. If the author retains the copyright, permission to copy must be obtained from the author.

Unless otherwise expressly stated, the views expressed herein are attributed to the author and not to this publication or URMIA. The materials appearing in this publication are for information purposes only and should not be considered legal or financial advice or used as such. For a specific legal or financial opinion, readers should confer with their own legal or financial counsel.

UNIVERSITY RISK MANAGEMENT &
INSURANCE ASSOCIATION

URMIA National Office
P.O. Box 1027
Bloomington, Indiana 47402
www.urmia.org