AN A.S. PRATT PUBLICATION
MAY 2021
VOL. 7 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 4** **MAY 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Fines for HIPAA Security Rule Violations Found Unjustified by Fifth Circuit

By Jami Mills Vibbert, Nancy L. Perkins, Alex Altman, and Jason T. Raylesberg*

The U.S. Court of Appeals for the Fifth Circuit has vacated a $4,348,000 penalty imposed on the University of Texas MD Anderson Cancer Center for alleged violations of the privacy and security regulations. The authors of this article explain the decision, which highlights the important distinction between violations of privacy or security mandates or standards and the occurrence of security breaches.

A three-member panel for the U.S. Court of Appeals for the Fifth Circuit has unanimously vacated a $4,348,000 penalty that the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS") imposed on the University of Texas MD Anderson Cancer Center ("MD Anderson") for alleged violations of the privacy and security regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").

BACKGROUND

The case arose from three incidents that occurred in 2012 and 2013 in which, respectively, an MD Anderson faculty member had his or her laptop stolen and an MD Anderson trainee and visiting researcher each lost the USB thumb drive in their possession. Each of these devices were unencrypted, and collectively they contained electronic protected health information ("PHI") concerning nearly 35,000 individuals.

Despite the vast amount of PHI involved, the Fifth Circuit found that MD Anderson did not violate either the HIPAA security requirements ("Security Rule") or the privacy requirements ("Privacy Rule") invoked by OCR, and that the civil monetary penalty imposed by OCR was "arbitrary, capricious and otherwise unlawful." The court remanded the case to the agency for further proceedings.

THE DECISION

OCR's contention under the Security Rule was that MD Anderson violated the Rule's requirement to "[i]mplement a mechanism to encrypt" PHI or adopt some other

* Jami Mills Vibbert (jami.vibbert@arnoldporter.com) is a partner at Arnold & Porter Kaye Scholer LLP helping clients navigate global data protection, privacy, and cybersecurity concerns across a number of industries, including life sciences, healthcare, financial services, media, and technology. Nancy L. Perkins (nancy.perkins@arnoldporter.com) is counsel at the firm focusing her practice on regulatory compliance and consulting on emerging policy issues, with a principal focus on data privacy and security and electronic transactions. Alex Altman (alexander.altman@arnoldporter.com) is a senior associate at the firm concentrating his practice in global data protection, privacy, and cybersecurity matters. Jason T. Raylesberg (jason.raylesberg@arnoldporter.com) is an associate at the firm advising clients on a variety of data privacy and security issues.

"reasonable and appropriate method to limit access to patient data," as indicated by the aforementioned security breaches. But the court found to the contrary, noting that the Security Rule does not require "bulletproof protection" of PHI but rather requires entities subject to the Rule implement a "mechanism" to encrypt PHI. In fact, the Security Rule's encryption standard is an "addressable" standard, not a "required" standard, meaning that it is to be implemented "if reasonable and appropriate" as determined by the regulated entity.

The Fifth Circuit found that MD Anderson complied with this standard by, for example, requiring employees to adhere to an "Information Resources Acceptable Use Agreement and User Acknowledgment for Employees" that specified any PHI stored on portable computing devices "must be encrypted and backed up to a network server for recovery in the event of a disaster or loss of information." Further, MD Anderson provided employees with an "IronKey" to encrypt and decrypt mobile devices and implemented mechanisms for file-level encryption in its electronic health record software then in place, ClinicStation. In the court's view, whether MD Anderson failed to enforce these mechanisms rigorously enough is a separate question not within the ambit of the Security Rule's encryption standard.

With respect to the Privacy Rule, which generally prohibits a HIPAA covered entity from disclosing PHI without the written authorization of the individual to whom the PHI pertains, the court examined the meaning of "disclosure" for Privacy Rule purposes, which is "the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information." Underscoring that each verb used in this definition implies an "affirmative act of disclosure" as opposed to a "passive loss of information," the court disagreed with the notion that an "entity affirmatively acts to disclose information when someone steals it."

Moreover, the Fifth Circuit explained that the Privacy Rule definition of "disclosure" entails information be made known to someone outside of the covered entity, which the government conceded it could not show occurred in this case.

Citing a "bedrock principle of administrative law that an agency must 'treat like cases alike,'" the court also found that MD Anderson's financial punishment was in stark contrast to the absence of monetary penalties other covered entities faced for allegedly violating OCR's same interpretation of the Security Rule's encryption standard. For example, in response to Cedars-Sinai Health System's notification to OCR that an employee's unencrypted laptop was stolen in a residential burglary, OCR assessed no penalty, even though the laptop contained the PHI of more than 33,000 individuals.

Similarly, HHS assessed no penalties in response to a 2015 case in which North East Medical Services reported the theft of a workforce member's unencrypted laptop that stored PHI associated with more than 69,000 individuals, as well as a 2013 case in which AHMC Healthcare Inc. reported the theft from an office of two unencrypted

laptops containing PHI of 729,000 individuals. While the court agreed with OCR that each case presents a fact-specific inquiry, it noted this does not give the government the power to arrive at disparate conclusions on cases that present substantially similar sets of facts. Doing so, the court cautioned, would mean "an agency could give free passes to its friends and hammer its enemies – while also maintaining that its decisions are judicially unreviewable because each case is unique."

In addition to vacating OCR's penalty on these grounds, the Fifth Circuit pointed out that the penalty considerably exceeded the $100,000 per-year statutory cap set by Congress for violations attributable to "reasonable cause." Under the HITECH Act, OCR is authorized to impose civil monetary penalties of gradated amounts, by tiers corresponding to a covered entity's level of culpability in engaging in a violation, including violations with "reasonable cause" — i.e., "an act or omission in which a [regulated entity] knew, or by exercising reasonable diligence would have known, the act or omission violated an administrative simplification provision, but in which the [regulated entity] did not act with willful neglect."

In *MD Anderson*, despite the aforementioned $100,000 per year cap on penalties for such violations, OCR had applied the highest annual limit of $1,500,000 to all categories of violations on the basis that this was "consistent with Congress' intent to strengthen enforcement." OCR itself recognized, in a "Notice of Enforcement Discretion Regarding HIPAA Civil Monetary Penalties" published two months after the Departmental Appeals Board's decision in *MD Anderson,* that "upon further review of the statute by the HHS Office of the General Counsel, HHS has determined that the better reading of the HITECH Act" is to apply the annual limits precisely as set forth in the Act.

CONCLUSION

This Fifth Circuit decision highlights the important distinction between violations of privacy or security mandates or standards and the occurrence of security breaches. The law does not prohibit a security breach, at least as "security breach" is commonly defined in privacy laws, as legislatures recognize that the occurrence of security breaches is frequently beyond regulated entities' control. Instead, the law mandates that regulated entities implement reasonable and appropriate security safeguards.

OCR's allegations in *MD Anderson* appeared to blur this distinction, by suggesting that imperfect implementation of encryption mechanisms that led to unintended loss of PHI was a legal violation, as opposed to focusing on a failure to implement reasonable encryption mechanisms with reasonable care, which the Fifth Circuit found MD Anderson had done. The court's decision may cause OCR to realign its enforcement approach, as well as to exercise its enforcement discretion in a manner that results in more parity among penalties imposed in different cases presenting similar facts.