AN A.S. PRATT PUBLICATION
SEPTEMBER 2017
VOL. 3 • NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 7 SEPTEMBER 2017

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [233] (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

(2017–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, 718.224.2258. 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.

Could Your Patient Be "Wanted?" Taking Action Under HIPAA

By Sherry A. Fabina-Abney and Deepali Doddi*

A covered entity may report limited protected health information about potential criminal suspects to the local police or other law enforcement agencies in response to a request relayed by news outlets without running afoul of the HIPAA Privacy Rule. The authors of this article discuss the law enforcement exceptions to the Privacy Rule.

News and media alerts often convey law enforcement officials' requests for information about the identity of a suspected criminal. With the increasing rigor of enforcement activity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") by the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") and the recent uptick in privacy litigation, health care providers are often hesitant to share health information about their patients when presented with this unusual circumstance. But it is important to remember that the HIPAA Privacy Rule does not create inordinate barriers to the disclosure of protected health information ("PHI") in situations where the release of such information is vital to ensuring public safety.

HIPAA PRIVACY RULE

As OCR observes in its guidance on disclosures to law enforcement,[1] the Privacy Rule balances patients' interest in privacy with the need for effective law enforcement. To that end, the Privacy Rule permits a HIPAA covered entity to disclose PHI without patient authorization for various law enforcement purposes, such as to comply with court orders, subpoenas, and administrative requests, respond to requests about crime victims and criminal suspects, and report abuse, neglect, and certain criminal activities.

LAW ENFORCEMENT EXCEPTIONS

If a covered entity sees such a news report and believes one of its patients fits the suspect's profile, then the Privacy Rule permits the covered entity to share limited information about the patient with law enforcement officials without the patient's authorization. In particular, the Privacy Rule states that "a covered entity may disclose

* Sherry Fabina-Abney is a partner in the health law group at Ice Miller LLP serving clients with medical staff, peer review, license and accreditation, and physician-related issues and litigation. Deepali Doddi is an associate in the firm's Data Security and Privacy practice, advising regulated entities regarding best practices for safeguarding data and ensuring compliance with the HIPAA Privacy and Security Rules and the Breach Notification Rule. The authors may be reached at sherry.fabina-abney@icemiller.com and deepali.doddi@icemiller.com, respectively.

[1] https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html.

[PHI] in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person."[2]

Under such circumstances, the request from law enforcement need not be directed specifically to the covered entity. The law enforcement request may take the form of a general request to the public, and the request may be issued through the media. Moreover, the law enforcement request need not be in writing. In its commentary to the 2000 Final Privacy Rule, OCR explained:

> We clarify our intent not to allow covered entities to initiate disclosures of limited identifying information to law enforcement in the absence of a law enforcement request; a covered entity may disclose protected health information under this provision only in response to a request from law enforcement. We allow a "law enforcement official's request" to be made orally or in writing, and we intend for it to include requests by a person acting on behalf of law enforcement, for example, requests by a media organization making a television or radio announcement seeking the public's assistance in identifying a suspect. Such a request also may include a "Wanted" poster and similar postings.[3]

If a covered entity chooses to report a patient to law enforcement officials as a possible criminal suspect, it must ensure that the identifying information it shares is limited in scope.[4] Namely, the covered entity may disclose only the following facts about the suspect to law enforcement officials: name and address; date and place of birth; Social Security number; ABO blood type and Rh factor; type of injury; date and time of treatment; date and time of death, if applicable; and a description of the patient's distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, facial hair, scars, and tattoos.[5] The covered entity cannot share information related to the suspect's DNA or DNA analysis, dental records, or samples or analysis of body fluids or tissue.[6] Nor may the covered entity disclose specific clinical or diagnostic information to law enforcement officials, aside from the general types of injuries the suspect may have experienced.

A covered entity should also remember to document such a disclosure to law enforcement officials in its accounting of disclosures of the patient's PHI, unless law enforcement officials provide the covered entity with a written statement that an

---

[2] *See* 45 C.F.R. § 164.512(f)(2).

[3] *See* Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462, 82531 (December 28, 2000).

[4] A workforce member who has a suspicion that a patient may be a criminal suspect is advised to confer with the covered entity's privacy officer or in-house legal department prior to discussing the patient's information with law enforcement officials.

[5] *See* 45 C.F.R. § 164.512(f)(2)(i).

[6] *See* 45 C.F.R. § 164.512(f)(2)(ii).

accounting to the patient would be reasonably likely to impede law enforcement activities and specifying the time period for which such an accounting cannot be provided to the patient.[7]

CONCLUSION

Accordingly, a covered entity may report limited PHI about potential criminal suspects to the local police or other law enforcement agencies in response to a request relayed by news outlets without running afoul of the HIPAA Privacy Rule.[8] OCR recognizes that certain disclosures of patient information are necessary for law enforcement operations to function smoothly and has acknowledged that "when only limited identifying information is disclosed and the purpose is solely to ascertain the identity of a [suspect], the invasion of privacy would be outweighed by the public interest."[9]

[7] *See* 45 C.F.R. § 164.528(a).

[8] Nevertheless, a covered entity should evaluate whether such a disclosure to law enforcement is permitted under applicable state laws, which may contain more stringent requirements than the HIPAA Privacy Rule. Further, health care providers with federally-assisted drug and alcohol abuse programs (i.e., "Part 2" programs) should consider whether such a disclosure to law enforcement about a patient who receives treatment for substance abuse is consistent with the Confidentiality of Alcohol and Drug Abuse Patient Records regulations at 42 C.F.R. Part 2.

[9] *See* Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59918, 59962 (November 3, 1999).