AN A.S. PRATT PUBLICATION
FEBRUARY/MARCH 2021
VOL. 7 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 2** **February/March 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.

Data Breaches and HIPAA Enforcement Remain Widespread Amidst the COVID-19 Pandemic

By Michelle Capezza and Alaap B. Shah*

The authors of this article discuss two Office for Civil Rights data breach-related settlements, one from a HIPAA Covered Entity and one from a HIPAA Business Associate, the lessons learned, and best practices for organizations to follow.

In September 2020, the Office for Civil Rights ("OCR") at the U.S. Department of Health and Human Services ("HHS"), the agency enforcing the Health Insurance Portability and Accountability Act ("HIPAA") Privacy, Security, and Breach Notification Rules, obtained two large breach-related settlements: one from a HIPAA Covered Entity and one from a HIPAA Business Associate. These enforcement actions signal that despite COVID-19 related challenges, organizations continue to face rampant data breaches and ensuing HIPAA enforcement.

THE SETTLEMENTS

The OCR settled an investigation into a breach suffered by a large health insurer by obtaining the second-largest resolution payment in HIPAA enforcement history ($6.85 million).[1] This enforcement action resolved an investigation concerning potential violations of HIPAA Privacy and Security Rules related to a breach affecting the electronic protected health information ("ePHI") of more than 10.4 million people. The breach resulted from a phishing attack that introduced malware into the insurer's IT systems and allowed unauthorized actors to gain access and remain undetected for nearly nine months.

Similarly, a business associate providing IT and health information management services to hospitals and physicians clinics entered a settlement ($2.3 million)[2] with OCR for potential violations of HIPAA Privacy and Security Rules related to a breach affecting over six million people.

Essentially, these cyberattacks were advanced persistent threats that compromised the privacy and security of ePHI and PHI and revealed longstanding gaps in the companies' cybersecurity controls.

---

* Michelle Capezza is a member of the firm at Epstein Becker & Green, P.C., in the Employee Benefits & Executive Compensation and Health Care & Life Sciences practices. Alaap B. Shah is a member of the firm in the Health Care and Life Sciences practice. The authors may be reached at mcapezza@ebglaw.com and abshah@ebglaw.com, respectively.

[1] https://www.hhs.gov/sites/default/files/premera-ra-cap.pdf.

[2] https://www.hhs.gov/sites/default/files/chspsc-ra-cap.pdf.

LESSONS LEARNED

The parties in both of these cases entered into comprehensive Resolution Agreements and Corrective Action Plans. These settlement documents provide an informative checklist of considerations for similar entities to implement as proactive as well as reactive measures. In particular, these Corrective Action Plans stressed the importance of implementing proactive policies, procedures and training around access controls. OCR also required augmenting reactive policies and procedures relating to auditing and monitoring system activity. Moreover, the incidents also serve as a reminder for all organizations regarding the importance of engaging in an enterprise-wide risk analysis around cybersecurity, and implementation of risk management and controls measures. In fact, these Corrective Action Plans included requirements to conduct such risk analyses and implement risk management plans accordingly.

It is also worth noting that on January 5, 2021, H.R. 7898 was signed into law to amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of HHS to consider certain recognized security practices of covered entities and business associates when making determinations related to HIPAA fines, audits or mitigation remedies. This prospect of reducing risk of regulatory enforcement serves as an increased motivation to ensure recognized cybersecurity practices are in place now.

BIG PICTURE VIEW ON BEST PRACTICES

Although OCR's enforcement authority is limited to HIPAA, it is critical to note that enterprise-wide risk analyses should account not only for PHI, but also for other personally identifiable information ("PII"). Nearly every organization will possess PII, and nearly every healthcare entity will possess PHI and PII, with each bearing privacy and security obligations under a variety of federal laws and regulations (beyond HIPAA) specifically addressing cybersecurity practices (such as the Gramm-Leach-Bliley Act of 1999, the Federal Trade Commission Act of 1914, and Securities and Exchange Commission Regulation S-P).

Organizations must also be mindful of state and local requirements concerning cybersecurity, such as the NY SHIELD Act[3] or the California Consumer Privacy Act ("CCPA"),[4] as well as possible international considerations (e.g., General Data Protection Regulation ("GDPR")). Further, these requirements will continue to evolve as additional laws are passed or amended. For example, last November, California voters passed Proposition 24 (the California Privacy Rights and Enforcement Act ("CPRA")),

[3] https://www.healthlawadvisor.com/2020/02/28/annual-breach-reporting-required-under-ny-shield-act-for-some-health-care-companies/.

[4] https://www.healthlawadvisor.com/2020/08/21/ccpa-regulations-approved-by-the-ca-office-of-administrative-law/.

which will expand the CCPA, and among other things, establish an enforcement arm – the California Privacy Protection Agency – to defend consumer rights and extend enforcement including imposing penalties for negligence resulting in theft of consumers' emails and passwords.

In light of ever-present cyber risk and aggressive regulatory enforcement on many fronts, organizations should consider addressing the following in order to develop, or update their existing policies and procedures around cybersecurity and data breach response:

- *Assemble the Right Team.* There is not a one-size fits all approach to cybersecurity management. Depending on the size of your organization, data security may reside solely within the confines of the IT department's scope of responsibility or may extend upward all the way to executive leadership and the board.

  Regardless of organizational size, given the severity of potential risks and penalties associated with a cyber-breach, best practices involve establishing a dedicated team to develop cybersecurity policies and data breach response protocols. This team may be multi-disciplinary and include members from such areas as IT, risk management, legal, compliance, and human resources.

  The organization should commit to investing in robust data security software and hardware, and retain (where appropriate) outside service providers to assist with data protection efforts and incident response.

- *Prepare, Prepare, Prepare.* Cybersecurity programs are often only as strong as the workforce interacting with your organization's network. As such, it is imperative to implement robust cybersecurity training requirements for employees as well as security event notification processes related to phishing, ransomware, and other cyber threats.

  Yet even with the most robust training, given enough time, data breach becomes an inevitability. Thus, it is important for organizations to know who to contact in the event of breach, when to bring in law enforcement agencies, when to notify the organization's governing body, and government agencies.

  Likewise, it is critical to designate "on-call" members of the team to support in the context of a security event. This should include coverage schedules for off-hours and specific holidays to ensure that a member of the team is available to lead a response in the event of a cyber-breach. The team should also conduct tabletop testing exercises to prepare response coordination. By preparing to respond to a breach, organizations can ensure that damage will be contained as efficiently and effectively as possible. These "people and process" exercises should be done in tandem with robust "technology" testing such as penetration testing, vulnerability scanning, and other contingency planning.

- *Conduct a Risk Assessment.* A risk assessment is the first critical step in a cybersecurity compliance plan to identify the vulnerabilities in the organization's system. The HIPAA Security rule specifically requires conducting them.

  Further, The National Institute of Standards and Technology ("NIST") has placed great emphasis on conducting a risk assessment as the foundation for data security.

  As part of this assessment, an organization should also be able to identify the types of data that it collects, stores, and transmits in order to properly secure it and address data retention policies in accordance with applicable laws. Guidance on how to conduct these exercises is available in NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.[5]

- *Implement and Update Audit Controls.* Audit controls give a company visibility into their systems, allowing them to recognize suspicious activity early in order to limit exposure and ultimately prevent full-blown data breach. HIPAA requires audit controls to ensure entities have sufficient awareness about system activity (and specifically malicious activity).

  Further, HIPAA requires organizations to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use e-PHI. NIST audit control standards[6] provide more granular guidance on conducting proactive system monitoring and activity logging. If reasonable and appropriate controls are put in place relative to these safeguards, companies can thwart hackers from gaining unauthorized access to e-PHI.

- *Implement and Update Cybersecurity Policies.* As the cyber threat landscape continues to evolve, and novel federal and state requirements come online, it is prudent to ensure that your organization's policies and procedures are reasonable and appropriate and comport with best practices.

  Your organization should also ensure vendor cyber risk is managed through due diligence and robust contractual obligations such as data privacy and protection agreements. To the extent your organization collects data that is subject to the GDPR, a Data Protection Impact Assessment ought to be performed relating to personal data collection, maintenance and processing activities.

  Finally, your organization should also review its cyber liability insurance policies to ensure you have adequate "rainy day" coverage and funds in case

[5] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[6] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

a data breach, or the resulting regulatory obligations or enforcement, require significant capital outlays.

CONCLUSION

The time is now for all organizations to ensure that the proper cybersecurity policies and procedures and data breach response plans are in place and implemented enterprise-wide. Many of these activities require significant time and resource investments coupled with expert guidance from cybersecurity professionals.

Further, many of these activities (particularly risk analyses and tabletop exercises) surface compliance gaps and carry compliance implications.

As such, it is prudent to conduct such activities under attorney-client privilege to ensure the right compliance documentation is generated, while the "bad paper" identifying negative findings are protected from discovery.