PRACTICE RESOURCE

Health Care Data Breaches: Practical Advice for Trying Times

Kristen Rosati and Scott Bennett

What is the issue? Health care organizations and their business associates are increasingly vulnerable to data breaches. The causes of breaches range from simple human error to intentional theft and hacking incidents.

What is at stake? Dealing with a data breach is expensive, especially for health care organizations because of the extensive breach-reporting requirements of the Health Insurance Portability and Accountability Act and state breach laws. Breaches can also lead to extensive (and expensive) government investigations, fines, civil lawsuits, and the loss of customers and business reputation.

What should attorneys do? Having a good security risk management program and incident response plan in place will reduce the potential costs of a breach. In this Practice Resource, the authors provide practical suggestions for effective breach planning and response.

CITATION: Kristen Rosati and Scott Bennett, *Health Care Data Breaches: Practical Advice for Trying Times*, J. Health & Life Sci. L., Feb. 2017, at 90, © 2017 American Health Lawyers Association, www.healthlawyers.org/journal. All rights reserved.

Author biographies appear on the next page.

Kristen Rosati is a Partner at Coppersmith Brockelman. She is considered one of the nation's leading HIPAA compliance attorneys and has deep expertise with large data breaches, health information exchange, data sharing for research and clinical integration initiatives, electronic health record roll-outs, clinical research compliance and contracting, biobanking, and all matters related to "Big Data." Contact her via email at krosati@cblawyers.com.

Scott Bennett is a Partner at Coppersmith Brockelman, where his practice focuses on representing hospitals and other health care providers. He has helped many health care clients respond to—and mitigate the potential harm from—data breaches. He also has significant experience conducting internal investigations and representing clients in government investigations, criminal and civil litigation, and administrative proceedings. Contact him via email at sbennett@cblawyers.com.

Rosati and Bennett: Data Breaches

CONTENTS

Introduction

According to a study released in May 2016, nearly 90% of health care organizations surveyed had experienced a data breach in the past two years, and 45% had dealt with more than five breaches in the same time period.[1] The average estimated cost of a breach for a health care organization is $2.2 million.[2] For a business associate, the estimated cost is more than $1 million.[3] Breaches cost the health care industry an estimated $6.2 billion every year.[4]

The costs of a breach are higher in health care than in other industries, presumably because of the breach-reporting requirements of the Health Insurance Portability and Accountability Act (HIPAA). A study released in June 2016 found that the average cost of a data breach in the United States was $221 per compromised record; but for health care breaches, it was $355 per record.[5]

The number of patients affected by health care breaches is staggering. In 2015, the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS), the federal agency responsible for enforcing HIPAA, was notified of 253 breaches that collectively involved more than 112 million records.[6]

A data breach represents a significant problem that all organizations must be prepared to handle. The potential consequences include

[1] Ponemon Inst., Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data 1 (2016), *available at* www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm_source=Referral&utm_medium=press%20release&utm_campaign=Ponemon%202016 [hereinafter Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data].

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Ponemon Inst., 2016 Cost of Data Breach Study: Global Analysis 5, 10 (2016), *available at* www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN [hereinafter 2016 Cost of Data Breach Study].

[6] Dan Munro, *Data Breaches in Healthcare Totaled Over 112 Million Records In 2015*, Forbes (Dec. 31, 2015, 9:11 PM), www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#731780157fd5.

government investigations and fines, lawsuits by affected individuals, financial harm, customer loss, and reputational injury. Research suggests, however, that by taking steps to prevent and prepare for a breach, organizations can meaningfully reduce those costs.[7]

This Practice Resource will explain HIPAA's breach-reporting requirements, as well as address the requirements of state breach laws. The Practice Resource then provides specific suggestions that companies can follow to prepare for and respond to breaches.

The authors conclude that the health care industry regulators should examine whether breach-reporting requirements should be changed. Health care companies already are operating on a thin profit margin, and the substantial expense of reporting may force some of those companies out of business. More practical alternatives might protect individuals by requiring individual authentication for obtaining credit and other services, and instituting smarter payment algorithms to catch fraudulent claims. Ultimately, what would help consumers most is a system that requires reporting in those situations where individuals need to know about the breach to protect themselves.

HIPAA's Breach Reporting Requirements

The terms "security incident" and "breach" have specific definitions under HIPAA. Although a security incident generally means "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices,"[8] the HIPAA definition is more specific: "Security incident means the attempted or successful unauthor-

[7] Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, at 2.

[8] Nat'l Inst. of Standards & Tech., Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology 6 (2012), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. *See also* Rick Kam, *What's in a Name? Defining Event vs. Security Incident vs. Data Breach*, ID Experts Blog, Jul. 8, 2015, www2.idexpertscorp.com/blog/single/whats-in-a-name-defining-event-vs.-security-incident-vs.-data-breach.