



AHLA

# JOURNAL OF HEALTH & LIFE SCIENCES LAW

VOLUME 10, NUMBER 2

FEBRUARY 2017

## BRIEF INSIGHT

The Trump Administration and Antitrust Challenges  
to Hospital Mergers ..... 1  
*John J. Miles*

## FEATURE ARTICLE

The Use of Self-Critical Material as Adverse Evidence:  
Can Privilege Protect Against a Hobson's Choice? ..... 9  
*Scott R. Grubman*

## NOTES AND COMMENTS

Five Years After *NFIB*: Is Medicaid Expansion Still  
Feasible?..... 36  
*Jeffery Rowe*

The Yates Memo and the Push for Individual  
Accountability ..... 67  
*Jonathan S. Feld and Eric S. Klein*

## PRACTICE RESOURCE

Health Care Data Breaches: Practical Advice  
for Trying Times..... 90  
*Kristen Rosati and Scott Bennett*



OFFICIAL JOURNAL OF AMERICAN HEALTH LAWYERS ASSOCIATION

The mission of the AHLA *Journal of Health & Life Sciences Law* is to publish in-depth, professionally reviewed articles that are interesting and useful to intermediate and advanced health lawyers throughout the United States.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher and authors are not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

—from a declaration of the American Bar Association

Consistent with the American Health Lawyers Association's educational mission, it is an objective of the AHLA *Journal of Health & Life Sciences Law* to be a forum for the free expression and interchange of ideas. Contributors to the *Journal* are not agents of the American Health Lawyers Association. The opinions and positions stated in the *Journal* are those of the authors and not of the American Health Lawyers Association, its staff, volunteers, editors, or editorial board.

The AHLA *Journal of Health & Life Sciences Law* (ISBN 978-1-4224-4585-3. ISSN 1942-4736) is published three times per year by the American Health Lawyers Association, 1620 Eye Street, NW, 6th Floor, Washington, DC, 20006-4010. Telephone: 202-833-1100. [www.healthlawyers.org](http://www.healthlawyers.org).

© Copyright 2017 by the American Health Lawyers Association. All rights reserved. No part of this publication may be reproduced in any form except by prior written permission from the publisher. Produced in the United States of America.

The reprint of American Health Lawyers Association publications (including the *Journal of Health & Life Sciences Law*) for academic purposes is handled by the Copyright Clearance Center, [www.copyright.com](http://www.copyright.com), or 978-750-8400. To request reprint permission for other purposes (which will be addressed on a case-by-case basis), please contact Cynthia Conner at [cconner@healthlawyers.org](mailto:cconner@healthlawyers.org). In your request, please state the purpose of the reprint (e.g., if the material will be used as part of a seminar presentation, the name, date, sponsoring group, and location of the seminar), the anticipated number of copies to be generated, and whether the material will be made available for sale.

Subscriptions to the AHLA *Journal of Health & Life Sciences Law* are complimentary for members of the American Health Lawyers Association. Paid subscriptions are available at [www.healthlawyers.org/journal](http://www.healthlawyers.org/journal).



# From the EDITOR in CHIEF

Colleagues:

In this issue, our contributors explore several federal enforcement topics. Scott R. Grubman's Feature Article will resonate with providers seeking to ensure they have effective compliance plans. He asks, "[The Use of Self-Critical Material as Adverse Evidence: Can Privilege Protect Against a Hobson's Choice?](#)" Jonathan S. Feld and Eric S. Klein add to the dilemma in their Comment on [The Yates Memo and the Push for Individual Accountability](#).

In a Note, Jeffery Rowe asks, "[Five Years After NFIB: Is Medicaid Expansion Still Feasible?](#)" Every reader will want to download and save our Practice Resource: [Health Care Data Breaches: Practical Advice for Trying Times](#), authored by Kristen Rosati and Scott Bennett. Completing the issue as the new year unfolds, John J. Miles provides a Brief Insight exploring [The Trump Administration and Antitrust Challenges to Hospital Mergers](#).

We hope these articles provide useful and thought-provoking content in this time of federal transition. We welcome your feedback and questions at [journal@healthlawyers.org](mailto:journal@healthlawyers.org).

Sincerely,



Cynthia F. Wisner

Editor in Chief, *Journal of Health & Life Sciences Law*

# 2016–2017 Editorial Board

## AHLA Journal of Health & Life Sciences Law

**Cynthia F. Wisner**

Editor in Chief, *AHLA Journal of Health & Life Sciences Law*  
Associate Counsel, Trinity Health

**Elise Dunitz Brennan**

Conner & Winters LLP

**Michael H. Cook**

Liles Parker PLLC

**Richard G. Cowart**

Baker Donelson Bearman Caldwell & Berkowitz PC

**Lawrence L. Foust**

Children's Health System of Texas

**Lucy C. Hodder**

University of New Hampshire

**Travis G. Lloyd**

Bradley Arant Boult Cummings LLP

**Holley Thames Lutz**

Dentons US LLP

**Thomas Wm. Mayo**

Haynes and Boone LLP

**Jordan Paradise**

Loyola University Chicago School of Law

**Dorthula H. Powell-Woodson**

Wiley Rein LLP

**Cynthia Ransburg-Brown**

UAB Health System

**Susan O. Scheutzow**

Kohrman Jackson & Krantz PLL

**Paul W. Shaw**

Verrill Dana LLP

**Richard F. Tompkins**

First Chesapeake Group

# AHLA Journal of Health & Life Sciences Law

## Publication Staff

### David S. Cade

Executive Vice President/  
Chief Executive Officer  
American Health Lawyers Association  
[dcade@healthlawyers.org](mailto:dcade@healthlawyers.org)

### Cynthia Conner

Vice President of Professional Resources  
American Health Lawyers Association  
[cconner@healthlawyers.org](mailto:cconner@healthlawyers.org)

### William B. Harvey

Director of Business  
Development & Publishing  
American Health Lawyers Association  
[wharvey@healthlawyers.org](mailto:wharvey@healthlawyers.org)

### Kara Kinney Cartwright

Managing Editor  
*Journal of Health & Life Sciences Law*  
[kinneycartwright@comcast.net](mailto:kinneycartwright@comcast.net)

### Annie Hsu Shieh

Citation Editor

### Katherine E. Wone

Senior Legal Editor  
American Health Lawyers Association  
[kwone@healthlawyers.org](mailto:kwone@healthlawyers.org)

### Mary Boutsikaris

Creative Director  
American Health Lawyers Association  
[mboutsik@healthlawyers.org](mailto:mboutsik@healthlawyers.org)

## Association Professional Resources Committee

### John R. Holdenried, Chair

Mark A. Bonanno

Todd M. Ebersole

Toby G. Singer

James W. Boswell

Hal McCard

Thomas N. Shorter

## Association Board of Directors–Officers

### Charlene L. McGinty

President

### Eric Zimmerman

President-Elect

### Marilyn Lamar

President-Elect Designate

*This page intentionally left blank*

## The Trump Administration and Antitrust Challenges to Hospital Mergers

John J. Miles

Mergers of health care industry competitors, whether between hospitals, physicians, pharmaceutical manufacturers, health insurers, or others, have been rich antitrust targets for the Obama Administration. Nowhere has this been more true than in the hospital industry, where the Federal Trade Commission (FTC or Commission) began a winning streak shortly before Obama's 2008 election that has yet to end.<sup>1</sup>

Beginning with the FTC's 2007 decision in *Evanston Northwestern Healthcare Corporation*,<sup>2</sup> the FTC has won five major litigated hospital merger challenges.<sup>3</sup> Perhaps as important, several hospitals contemplating mergers abandoned their transactions in light of threatened or actual challenge.<sup>4</sup> Several other transactions were cleared only after

- 1 Two challenges were arguably unsuccessful, not because of the transactions' likely effect on competition but because, in one case, of the impossibility of divestiture given the state's certificate-of-need laws. See STATEMENT OF THE FEDERAL TRADE COMMISSION IN THE MATTER OF PHOEBE PUTNEY HEALTH SYSTEM, INC. ET AL. DOCKET No. 9348 (Mar. 31, 2015), available at [www.ftc.gov/system/files/documents/public\\_statements/634181/150331phoebeputneycommstmt.pdf](http://www.ftc.gov/system/files/documents/public_statements/634181/150331phoebeputneycommstmt.pdf); and in the other case, because the state enacted a statute arguably providing the transaction with state-action exemption protection. See STATEMENT OF THE FEDERAL TRADE COMMISSION IN THE MATTER OF CABELL HUNTINGTON HOSPITAL, INC., DOCKET No. 9366 (July 6, 2016), available at [www.ftc.gov/system/files/documents/public\\_statements/969783/160706cabellcommstmt.pdf](http://www.ftc.gov/system/files/documents/public_statements/969783/160706cabellcommstmt.pdf).
- 2 In the Matter of Evanston Nw. Healthcare Corp., 144 F.T.C. 1, 381 (2007), available at [www.ftc.gov/system/files/documents/commission\\_decision\\_volumes/volume-144/vol144.pdf](http://www.ftc.gov/system/files/documents/commission_decision_volumes/volume-144/vol144.pdf).
- 3 In addition to *Evanston Northwestern Healthcare*, see *FTC v. Advocate Health Care Network*, 841 F.3d 460 (7th Cir., Oct. 31, 2016); *FTC v. Penn State Hershey Med. Ctr.*, 838 F.3d 327 (3d. Cir. 2016); *ProMedica Health Sys. v. FTC*, 749 F.3d 559 (6th Cir. 2014); *FTC v. OSF Healthcare Sys.*, 852 F. Supp. 2d 1069 (N.D. Ill. 2012).
- 4 See, e.g., In the Matter of Reading Health Sys., No. 9353 (FTC Dec. 12, 2012) (Order Dismissing Complaint in light of transaction abandonment), available at [www.ftc.gov/sites/default/files/documents/cases/2012/12/121207readingsircmpt.pdf](http://www.ftc.gov/sites/default/files/documents/cases/2012/12/121207readingsircmpt.pdf).

agreements to divest.<sup>5</sup> The most recently litigated challenges both focused on delineation of the geographic market; the hospitals won at the district court level, where courts refused to grant the FTC preliminary injunctions—only to lose on appeal. In *Hershey Medical Center*, the Third Circuit ordered the district court to grant the injunction. In *Advocate Health Care*, the Seventh Circuit remanded the case for further consideration by the district court. Hospitals and their counsel must be wondering whether the FTC will ever lose a hospital merger case.

The aggressiveness of the Obama Administration in antitrust matters surprised no one. Mr. Obama had stated during his campaign that he intended to “reinvigorate” antitrust enforcement, and he followed through. The election of Donald Trump raises the question whether the Trump Administration FTC will view hospital mergers more hospitably than the Obama Administration has. The question can’t be answered conclusively, but there are some reasons to believe that, at least at the margins, the answer is yes.

The Republican Platform is silent about antitrust, and Mr. Trump has issued no position papers addressing it. He has, in off-the-cuff remarks, indicated concern about industry concentration generally, voicing opposition to the proposed AT&T/Time Warner merger as an example and accusing Amazon of constituting a monopoly engaging in anticompetitive behavior.<sup>6</sup>

Suggesting a less aggressive approach, however, is his appointment of Joshua Wright as the transition guru in charge of antitrust.<sup>7</sup> Mr. Wright, a

---

5 See, e.g., In the Matter of Community Health Sys, Inc., No. C-4427 (FTC Apr. 11, 2014) (Decision and Order requiring hospital divestitures), available at [www.ftc.gov/system/files/documents/cases/140415chshmdo.pdf](http://www.ftc.gov/system/files/documents/cases/140415chshmdo.pdf).

6 See Brian Stelter, *Donald Trump Rips Into Possible AT&T-Time Warner Deal*, CNN MONEY (Oct. 22, 2016 4:05 PM), <http://money.cnn.com/2016/10/22/media/donald-trump-at-t-time-warner/>; Ryan Knutson, *Trump Says He Would Block AT&T-Time Warner Deal*, WALL ST. J. (Oct. 22, 2016 2:50 PM), [www.wsj.com/articles/trump-says-he-would-block-at-t-time-warner-deal-1477162214](http://www.wsj.com/articles/trump-says-he-would-block-at-t-time-warner-deal-1477162214).

7 See Leah Nysten, *Former FTC Commissioner Wright to Lead Trump Transition on Antitrust*, MLEX MARKET INSIGHT, Nov. 14, 2016, <http://mlexmarketinsight.com/editors-picks/former-ftc-commissioner-wright-lead-trump-transition-antitrust/>.



Ph.D. in economics, is a Republican, a law professor at the Antonin Scalia Law School of George Mason University, and an FTC Commissioner from 2013 to 2015. He was the most conservative of the five commissioners, dissenting from the Commission's decisions to challenge several mergers, and he is a strong believer of a strictly economic approach in analyzing antitrust issues. Mr. Wright will be heavily involved in choosing new FTC commissioners, as well as the Chairperson. Mr. Trump will likely appoint two Republicans, and possibly also a conservative Democrat or Independent. (No more than three commissioners may be of the same political party.)

What would that composition say about the Commission's likely aggressiveness in challenging hospital mergers? The best bet is that the Commission will turn slightly to the right, but any change in enforcement likely would be marginal. Antitrust enforcement historically has enjoyed bipartisan support with relatively little difference in enforcement philosophy. A review of Obama Administration FTC hospital merger challenges reveals nothing radical or outside mainstream antitrust analysis. The merging hospitals subject to those challenges were almost all close competitors or very good substitutes for each other, triggering concern that they could increase prices themselves post-merger—that the mergers would result in what the agencies' *Horizontal Merger Guidelines* refer to as anticompetitive “unilateral effects.”<sup>8</sup> In each challenge, the merging hospitals' post-merger market shares would have been extremely high, another danger signal. There seem to be, however, several areas of merger analysis that a Trump FTC might carefully examine. Two are the presumptive unlawfulness in “unilateral effects” cases based on the merger's effect on market concentration, and the analysis of efficiencies in rebutting a presumption of unlawfulness.

---

8 U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, HORIZONTAL MERGER GUIDELINES § 6 (2010), available at [www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf](http://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf) [hereinafter MERGER GUIDELINES].

Mergers between competitors primarily raise concerns about the likelihood of unilateral effects and/or coordinated effects. Unilateral effects occur when the merging firms raise prices regardless of the pricing behavior of other competitors, resulting from the loss of competition between the merging parties.<sup>9</sup> Coordinated effects occur when the merger results in a market sufficiently concentrated that it performs as an oligopoly—that the merged firms and their competitors raise their prices by engaging in interdependent competitive decision making through tacit agreement or conscious parallelism (but without an actual agreement that would violate Section 1 of the Sherman Act).<sup>10</sup> The theory is that the fewer the competitors, the easier and more likely it is that coordinated decision making will result. Thus far, every hospital merger challenge has relied primarily on concern about likely unilateral effects.<sup>11</sup>

Under the *Merger Guidelines*, a rebuttable presumption of likely anti-competitive effect (and thus unlawfulness) arises if a market's post-merger concentration level and the increase in concentration resulting exceed certain thresholds.<sup>12</sup> Based primarily on a 1963 Supreme Court opinion, the same is true if the merging parties' post-merger market share exceeds a certain level—30 percent.<sup>13</sup> The Trump Administration's approach to antitrust enforcement in health care, however, may rely less on this rebuttable presumption of unlawfulness because post-merger market concentration and the degree to which the merger increases that level provide little, if any, help in predicting the merger's effect on unilateral price increases.

Market concentration and the increase in concentration from the merger are obviously relevant—indeed the most important variables—in

---

9 *Id.* § 6.

10 *Id.* § 7 (“Coordinated interaction involves conduct by multiple firms that is profitable for each of them only as the result of the accommodating reactions of the others.”).

11 One challenge did involve both. See *FTC v. OSF Healthcare Sys.*, 852 F. Supp. 2d 1069, 1086–88 (N.D. Ill. 2012) (discussing coordinated effects).

12 *MERGER GUIDELINES* § 5.3.

13 *United States v. Philadelphia Nat'l Bank*, 374 U.S. 321, 364 (1963).

predicting whether a merger will result in *coordinated* effects. They predict little, however, about the merger's likely generation of *unilateral* effects. A post-merger market can be highly concentrated and yet the merging parties lack the ability to unilaterally raise prices. Indeed, the *Merger Guidelines* suggest this,<sup>14</sup> as do the agencies' *Commentary on the Horizontal Merger Guidelines*,<sup>15</sup> and leading commentators.<sup>16</sup> What is important is not concentration, but the degree of substitutability between the merging parties as opposed to their substitutability with other actual or potential competitors.<sup>17</sup> For example, assume a significant number of patients consider hospitals A and B very good substitutes—perhaps their first and second choices—but do not consider hospitals C, D, and E good alternatives. Health plans can threaten to exclude A and include B (or vice versa) if one of them demands what the plans consider excessive reimbursement. If A and B merge, however, this is not possible; the plans must either pay the merged hospital the higher reimbursement or risk losing subscribers because the other hospitals are unacceptable substitutes in their eyes.

Notwithstanding the irrelevance of market concentration in unilateral effects challenges to hospital mergers, up until now the agencies have continued to argue and the courts have continued to accept that

---

14 MERGER GUIDELINES § 6.1 ("The Agencies rely much more on the value of diverted sales than on the level of the HHI [i.e., market concentration] for diagnosing unilateral price effects . . .").

15 FTC & U.S. DEP'T OF JUSTICE, COMMENTARY ON THE MERGER GUIDELINES 16 (2006), available at [www.justice.gov/atr/file/801216/download](http://www.justice.gov/atr/file/801216/download) ("Indeed, market concentration may be unimportant under a unilateral effects theory of competitive harm . . . [T]he question in a unilateral effects analysis is whether the merged firm likely would exercise market power absent any coordinated response from rival market incumbents. The concentration of the remainder of the market often has little impact on the answer to this question.").

16 Carl Shapiro, *The 2010 Horizontal Merger Guidelines: From Hedgehog to Fox in Forty Years*, 77 ANTITRUST L. J. 49, 68 (2010) (noting that "HHI levels are of limited predictive value for this purpose" of assessing the potential for unilateral effects).

17 See MERGER GUIDELINES § 6.1 ("Substantial unilateral price elevation post-merger for a product formerly sold by one of the merging firms normally requires that a significant fraction of the customers purchasing that product view products formerly sold by the other merging party as their next-best choice.").

sufficient post-merger market concentration and increase prove a prima facie case.<sup>18</sup> Although the FTC introduces other supporting evidence—party “hot documents,” testimony about the merger’s effect from health plans, and econometric evidence—one would hope that a Trump Administration FTC would either explain the relationship between market concentration and unilateral effects or stop relying on concentration as its case in chief. If it does, the Trump FTC might well also examine the appropriateness of any rebuttable presumption of unlawfulness in any merger challenge, ultimately requiring the Commission to prove its case of actual or likely anticompetitive effects, just as a plaintiff must do in a Section 1 Sherman Act case.

Another area where a Trump FTC might diverge from the current approach, particularly in hospital merger investigations and challenges, is the assessment of efficiencies from the transaction and the burden that merging hospitals must meet to show that a transaction’s efficiencies offset its potential anticompetitive effects. The new administration should consider: Are there really situations in which the efficiencies from a transaction can offset its likely anticompetitive effects? If so, is the proof burden too stringent?

The *Merger Guidelines* provide that situations can arise in which the efficiency effects of a merger will offset its potential adverse effect on competition.<sup>19</sup> Commission officials have said the same in both speeches and articles.<sup>20</sup> And yet in complaints and briefs, the FTC emphasizes that no appellate court has ever held that an efficiencies claim rebutted a

---

18 See, e.g., *FTC v. Penn State Hershey Med. Ctr.*, 838 F.3d 327, 346 (3d Cir. 2016); *ProMedica Health Sys. v. FTC*, 749 F.3d 559, 568 (6th Cir. 2014).

19 *MERGER GUIDELINES* § 10 (“The Agencies will not challenge a merger if cognizable efficiencies are of a character and magnitude such that the merger is not likely to be anticompetitive in any relevant market.”).

20 See, e.g., Jeffrey H. Perry & Richard H. Cunningham, *Effective Defenses of Hospital Mergers in Concentrated Markets*, 27 *ANTITRUST* 43 (2013) (“When substantiated—meaning that the evidence supports the notion that a hospital merger will improve the quality of care at the affected hospitals—such claims may well carry the day, overcoming high market concentration levels, ‘hot documents,’ health plan concerns about a merger, and other factors that weigh in favor of enforcement.”).

prima facie case based on market concentration.<sup>21</sup> Hospitals and their attorneys thus wonder whether it is even worth their while to thoughtfully formulate and present a claim attempting to meet the *Merger Guidelines*' requirements for "cognizable efficiencies."<sup>22</sup>

A Trump Administration FTC may change this calculus, swinging the pendulum away from a disturbing possible interpretation of the Ninth Circuit's discussion of efficiencies in a successful challenge to St. Luke's Health System's acquisition of a large physician practice. There, the court held, or at least suggested, that better quality of care resulting from the merger would not constitute a cognizable efficiency because there was no evidence that it would improve competition.<sup>23</sup> A Trump FTC may be inclined to determine, however, that as long as competition is based in part on quality, quality improvements would inherently further competition without the necessity of direct proof of that effect. The benefits of these efficiencies, it follows, would be passed on to consumers as the *Merger Guidelines* and court decisions require.

Efficiency claims require predictions about both actions and results. Balancing efficiencies, particularly those relating to quality improvements, is difficult, and if the claimed efficiencies are not achieved, it may be difficult to "unscramble the eggs." But absent evidence of adverse effects on competition from a previously consummated merger, anticompetitive effects are predictive and speculative in any event. The

- 
- 21 See, e.g., Complaint at 16, In the Matter of Penn State Hershey Med. Ctr. & PinnacleHealth Sys., No. 9368 (FTC Dec. 7, 2015), available at [www.ftc.gov/system/files/documents/cases/151214hersheypinnaclecmpt.pdf](http://www.ftc.gov/system/files/documents/cases/151214hersheypinnaclecmpt.pdf) ("No court has ever found, without being reversed, that efficiencies rescue an otherwise illegal transaction.").
  - 22 MERGER GUIDELINES § 10 ("Cognizable efficiencies are merger-specific efficiencies that have been verified and do not arise from anticompetitive reductions in output or service.")
  - 23 St. Alphonsus Med. Ctr.—Nampa, Inc. v. St. Luke's Health Sys., 778 F.3d 775, 791 (9th Cir. 2015) ("It is not enough to show that the merger would allow St. Luke's to better serve patients . . . [T]he claimed efficiencies . . . must show that the prediction of anticompetitive effects from the prima facie case is inaccurate . . . [T]he [district court] judge did not find that the merger would increase competition or decrease prices.").

Trump FTC may want to study this problem to see if there is some middle ground to ensure that the efficiencies “defense” is not dead.

These are only two antitrust issues that may face the Trump Administration. More generally, it may be interesting to see the effect of the new administration on the Affordable Care Act and what ramifications any repeal, amendment, or replacement of the ACA might have on antitrust enforcement in the health care sector.

[Jeff Miles](#) is Senior Counsel in the Washington, D.C. office of Baker Donelson and limits his practice to health care antitrust matters. Contact him via email at [jmiles@bakerdonelson.com](mailto:jmiles@bakerdonelson.com).

## FEATURE ARTICLE

# The Use of Self-Critical Material as Adverse Evidence: Can Privilege Protect Against a Hobson's Choice?

Scott R. Grubman

**What is the issue?** A government investigation and/or a lawsuit alleging a violation of the False Claims Act can potentially obligate a health care provider to disclose self-critical material that was created as part of an internal investigation and/or self-audit conducted for purposes of ensuring compliance with government regulations.

**What is at stake?** The potential for disclosure presents the health care provider with a Hobson's choice of either investigating and correcting any violations while simultaneously creating a potentially self-incriminating record that may be used as evidence of liability, or avoiding fixing the problems and thereby leaving the provider open to liability.

**What should attorneys do?** Attorneys can help ensure protection of their clients' self-critical materials and avoid subsequent disclosure by structuring internal audits and investigations so that they are conducted at the direction of counsel and protected by attorney-client privilege.

**CITATION:** Scott R. Grubman, *The Use of Self-Critical Material as Adverse Evidence: Can Privilege Protect Against a Hobson's Choice?*, J. HEALTH & LIFE SCI. L., Feb. 2017 at 9. © 2017 American Health Lawyers Association, [www.healthlawyers.org/journal](http://www.healthlawyers.org/journal). All rights reserved.

*Author biography appears on the next page.*

[Scott R. Grubman](#) is a Partner at Chilivis, Cochran, Larkins & Bever. He represents health care providers in fraud and compliance matters, including government investigations and False Claims Act litigation. Mr. Grubman also serves as Adjunct Professor of Law at Emory University School of Law and Georgia State University College of Law, where he teaches health care fraud and abuse. Contact him via email at [sgrubman@cclblaw.com](mailto:sgrubman@cclblaw.com).



## **Grubman: Self-Critical Material as Adverse Evidence**

### **CONTENTS**

Introduction .....	12
OIG Guidance to Health Care Providers on Self-Audits and Reviews...	15
Discoverability of Self-Critical Material .....	17
Application of state peer review privileges .....	17
Application of the federal self-critical analysis privilege.....	22
Using Attorney-Client Privilege to Protect Self-Critical Material.....	26
Conclusion .....	34

## Introduction

In various guidance released over the years, the U.S. Department of Health and Human Services' Office of Inspector General (OIG) has repeatedly encouraged health care providers of all types and sizes to engage in regular audits and other types of internal, self-critical reviews to ensure compliance with the myriad rules and regulations governing the health care industry. For example, well over a decade ago, the OIG released a document entitled "OIG Compliance Program for Individual and Small Group Physician Practices," which touted the benefits of a voluntary compliance program, including the optimization of proper payments of claims, the minimization of billing mistakes, and reducing the chance of a government audit.<sup>1</sup> According to the OIG, the very first component of a physician practice's effective compliance program is "[c]onducting internal monitoring and auditing through the performance of periodic audits."<sup>2</sup> The OIG is not alone in encouraging physicians to engage in regular internal audits to ensure compliance; such reviews are essential to identifying existing issues and fixing them.<sup>3</sup>

Despite the potential rewards, engaging in self-critical analysis by way of an internal audit or investigation is not without risks. Often, as part of an investigation under the False Claims Act (FCA), the government will subpoena information from the investigation's target related to internal audits and reviews. In a recent OIG subpoena issued in an investigation with which the author is familiar, the government sought all "[d]ocuments that reflect, refer, or relate to any audits . . . including, but not limited to, final reports, recommendations, correspondence,

---

1 OIG Compliance Program for Individual and Small Group Physician Practices, 65 Fed. Reg. 59434, 59435 (Oct. 5, 2000), available at <https://oig.hhs.gov/authorities/docs/physician.pdf>.

2 *Id.* at 59436.

3 For example, the American College of Emergency Physicians recommends that compliance plans include "routine internal and external self-audits." ACEP REIMBURSEMENT COMM., ATTACHMENT A: PREPARING FOR PAYER AUDITS 12 (2016), available at [www.acep.org/uploaded-Files/ACEP/practiceResources/issuesByCategory/reimbursement/Preparing%20for%20Payer%20Audits.pdf](http://www.acep.org/uploaded-Files/ACEP/practiceResources/issuesByCategory/reimbursement/Preparing%20for%20Payer%20Audits.pdf).

memoranda, work papers, and interview notes, whether such audits were conducted internally or by an outside entity ... related to any procedures, services, or treatments provided by [the recipient healthcare practice].”<sup>4</sup>

By their very nature, these types of documents often offer candid self-assessments of any issues uncovered and specific remedial recommendations for moving forward. Indeed, these are the benefits promoted by encouraging health care providers to engage in regular internal audits in the first place. Yet, when these documents are in the hands of the government as part of an FCA investigation (or in the hands of an FCA relator as part of FCA litigation),<sup>5</sup> they have the potential to provide key evidence of an FCA violation, particularly as it relates to the FCA’s knowledge requirement, which requires proof that the defendant had actual knowledge or acted with reckless disregard or deliberate ignorance.<sup>6</sup> Put simply, when a health care provider follows best practices and conducts regular internal audits and reviews to improve internal processes and compliance, it might uncover evidence of billing errors material to payment that could form the basis of a government false claim allegation.

Outside the billing context, similar concerns have led state legislatures to create evidentiary privileges to encourage thorough and candid self-reviews related to patient care and safety. Specifically, many state legislatures have passed statutes expressly protecting peer review materials created by health care providers, exempting such materials from civil discovery.<sup>7</sup> Although there is no peer review privilege under federal law, federal courts often apply state privileges such as the peer review

---

4 On file with author.

5 The FCA permits private persons (known as “relators” under the statute) to serve as whistleblowers and bring suits in the name of the government alleging violations of the FCA. 31 U.S.C. § 3730(b).

6 *Id.* § 3729(b)(1).

7 See, e.g., GA. CODE ANN. § 31-7-133(a) (Georgia’s peer review statute, generally providing that “the proceedings and records of a review organization shall be held in confidence and shall not be subject to discovery or introduction into evidence in any civil action ...”).

privilege where doing so is not in conflict with “federal substantive and procedural policy.”<sup>8</sup>

Federal courts have also recognized a more generally applicable federal self-critical analysis privilege, which protects certain self-critical analyses from discovery when specific factors are met.<sup>9</sup> As one district court stated, the self-critical analysis privilege protects an organization or individual from the Hobson’s choice of aggressively investigating accidents or possible regulatory violations—ascertaining the causes and results and correcting any violations or dangerous conditions while simultaneously creating a potentially self-incriminating record that may be evidence of liability—or deliberately avoiding making a record on the subject and possibly leaving the public exposed to danger to lessen one’s risk of civil liability.<sup>10</sup>

Federal courts have thus far been reluctant to apply the state peer review and federal self-critical analysis privileges in FCA matters, however. As a result, the Hobson’s choice that these privileges were designed to prevent in other contexts remains a concern in the context of the FCA. This article will discuss these issues in greater detail, including measures that health care providers can take to protect self-critical analysis materials so that they can conduct regular internal reviews without fear that their peer review materials might be used or treated as adverse evidence later.

First, the article will discuss the [OIG’s guidance related to self-audits and reviews](#). Next, the article will discuss the [limits of state peer privilege](#)

---

8 *Mem’l Hosp. for McHenry Cty. v. Shadur*, 664 F.2d 1058, 1061 (7th Cir. 1981) [hereinafter *Mem’l Hosp. for McHenry Cty.*].

9 *See, e.g., United States ex rel. Sanders v. Allison Engine Co., Inc.*, 196 F.R.D. 310, 312 (S.D. Ohio 2000). The *Allison Engine* case eventually made its way to the Supreme Court of the United States, which held that the provision of the FCA prohibiting the making or use of a false record or statement in order to induce the government to pay or approve a claim requires that a defendant must intend that the government itself pay the claim. 553 U.S. 662 (2008). Subsequent to the Supreme Court’s decision, however, Congress passed the Fraud Enforcement and Recovery Act of 2009 (FERA), Pub. L. 111-21, which effectively reversed the Supreme Court’s decision in *Allison Engine* by eliminating the language on which it was decided.

10 *Reichhold Chems. v. Textron*, 157 F.R.D. 522, 524 (N.D. Fla. 1994).

and the federal self-critical analysis privilege as they relate to the discoverability of self-critical analysis in FCA matters. Finally, the article will discuss how providers and their counsel can maximize the protections of the privilege most likely to apply in FCA matters, i.e., the attorney-client privilege, toward reducing the unwanted disclosure of self-critical material generated by compliance audits.

## OIG Guidance to Health Care Providers on Self-Audits and Reviews

Self-critical analysis is of vital importance to health care industry compliance. Taking physician practices as an example, in a 2000 guidance document, the OIG states that an “ongoing evaluation process” is vital to ensuring compliance, and that “an audit is an excellent way for a physician practice to ascertain what, if any, problem areas exist and focus on the risk areas that are associated with those problems.”<sup>11</sup> The OIG recommended two types of reviews: a “standards and procedures review” and a “claims submission audit.”<sup>12</sup> The former entails periodically reviewing a medical practice’s standards and procedures “to determine if they are current and complete.”<sup>13</sup> If such a review shows that the practice’s standards and procedures are outdated, “they should be updated to reflect changes in Government regulations or compendiums generally relied upon by physicians and insurers (i.e., changes in [CPT] or [ICD codes].”<sup>14</sup> The latter entails a review of bills and medical records “for compliance with applicable coding, billing and documentation requirements.”<sup>15</sup> As part of such a claims submission audit, the OIG recommends utilizing the practice of “benchmarking,” where a baseline (or snapshot) is “used to enable a practice to judge over time its prog-

---

11 OIG Compliance Program for Individual and Small Group Physician Practices, 65 Fed. Reg. at 59437.

12 *Id.*

13 *Id.*

14 *Id.*

15 *Id.*

ress in reducing or eliminating potential areas of vulnerability,” which “allows a practice to chart its compliance efforts by showing a reduction or increase in the number of claims paid and denied.”<sup>16</sup> According to the OIG, such self-audits can be used to determine whether:

- Bills are accurately coded and accurately reflect the services provided (as documented in the medical records);
- Documentation is being completed correctly;
- Services or items provided are reasonable and necessary; and
- Any incentive for unnecessary services exist.<sup>17</sup>

After conducting a baseline audit, the OIG recommends that the provider conduct periodic audits “at least once each year to ensure that the compliance program is being followed.”<sup>18</sup> The OIG further states that “[o]ne of the most important components of a successful compliance audit protocol is an appropriate response when the physician practice identifies a problem.”<sup>19</sup>

In its guidance, the OIG expressly stated that “preserving information relating to identification of the problem is as important as preserving information that tracks the physician practice’s reaction to, and solution for, the issue.”<sup>20</sup> It is this very information, however, that can eventually serve as critical adverse evidence in subsequent investigation or litigation. For example, where a health care provider follows the OIG’s guidance, conducting a baseline coding audit and annual follow-up audits to ensure proper coding and track compliance, those documents will most often contain candid assessments of coding accuracy, which the government could potentially use in a subsequent FCA matter involving coding issues. Those documents could be crucial evidence, particularly where the government or a private relator attempts to establish what the provider

---

16 *Id.*

17 *Id.*

18 *Id.*

19 *Id.* at 59438.

20 *Id.*

knew, or should have known under the FCA's knowledge requirement. Although health care providers and their legal counsel have urged courts to extend certain privileges to these types of materials to avoid these concerns, courts have generally refused to do so, as discussed below.

## Discoverability of Self-Critical Material

The question arises, then, whether existing legal privileges may protect self-critical information from discovery, effectively easing the tension between incentives to perform self-analysis and the risk of liability under the FCA and other related statutes and regulations. Health care providers have attempted to invoke state peer review privileges and a federal self-critical analysis privilege, but courts have not been receptive.

### Application of state peer-review privileges

The peer review process, a mainstay of hospitals, serves to investigate possible instances of substandard care provided by physicians and determine its causes. It is not strictly analogous to compliance self-audits, in which various types of providers compare billing data against recognized benchmarks to assess coding accuracy and compliance with federal laws as described in the [OIG recommendations above](#). Although several courts have been asked to apply state peer review privileges in federal FCA matters, the author was able to find only one case where the court did so, although, as described below, that lone exception contained very specific facts not present in the typical FCA case. Thus, under the current state of the law, state peer review privileges offer little, if any, protection for a health care provider who wishes to engage in self-critical analysis but avoid creating self-critical material that might later become discoverable in a federal FCA matter.

An example of a typical case in which a provider seeks to extend state peer review protections to materials sought in a false claims action is *United*

*States ex rel. Roberts v. QHG of Indiana.*<sup>21</sup> In *Roberts*, the relators brought a qui tam action alleging that the defendants violated the FCA because a physician intentionally caused infants to remain in the neonatal intensive care unit longer than necessary to increase reimbursement.<sup>22</sup> The defendants filed a motion for a protective order related, in relevant part, to materials sought by the relators that could potentially inquire into the defendant hospital's process of evaluating and monitoring the qualifications and skills of the defendant physician. The defendants argued that these materials were privileged under Indiana's peer review statute.<sup>23</sup>

According to the court in *Roberts*, the Indiana peer review statute was "a comprehensive statute designed to create an atmosphere amenable to effective peer review, and thus foster an effective review of (and presumably improvements to) the state's health care, by ensuring the confidentiality of peer review materials."<sup>24</sup> The court first noted that the relators' complaint asserted *federal* claims under the FCA, thereby making Federal Rule of Evidence 501 applicable to addressing the defendants' privilege claim.<sup>25</sup> The court went on to state, however, that "federal courts should, as a matter of comity, consider the law of the state in which the case arises, and recognize the state's evidentiary privileges 'where this can be accomplished at not substantial cost to federal substantive and procedural policy.'"<sup>26</sup> According to the court, "a federal court should incorporate a state privilege only to the extent that privilege is consistent with the federal policies at issue in a case."<sup>27</sup>

---

21 United States *ex rel. Roberts v. QHG of Ind., Inc.*, No. 1:97-cv-174 (N.D. Ind. Oct. 8, 1998) (Cosbey, Mag. J.) [hereinafter *Roberts*].

22 *Id.*

23 *Id.*

24 *Id.* at n.3.

25 *Id.* Today, FRE 501 provides: "The common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless any of the following provides otherwise: the United States Constitution; a federal statute; or rules prescribed by the Supreme Court. But in a civil case, state law governs privilege regarding a claim or defense for which state law supplies the rule of decision. FED. R. EVID. 501.

26 *Roberts*, (quoting *Mem'l Hosp. for McHenry Cty.*, at 1061).

27 *Id.* (citations omitted).



The court engaged in a fact-specific analysis of whether Indiana's peer review privilege was consistent with federal law. Concluding that it was not, the court first noted that privileges generally "are not favored and, where recognized, must be narrowly construed."<sup>28</sup> The court stated that it was required to "weigh the need for truth against the importance of the relationship or policy sought to be furthered by the privilege, and the likelihood that recognition of the privilege will in fact protect that relationship in the factual setting of the case."<sup>29</sup> Applying those general principles to the specific facts before it, the court concluded that the need for full disclosure of the relevant evidence was substantial, and it discussed the strong public policy "embodied in the [FCA]" that would be vindicated if the relators were successful.<sup>30</sup> The court also noted that the information sought appeared to be "the only source of evidence from which the Relators could establish actual knowledge on the part of the Defendants, an element of proof required by the [FCA]."<sup>31</sup> "In other words," the court stated, "if the Relators were unable to access this information, they may very well be prevented from proving their [FCA] fraud claims."<sup>32</sup> The court continued, "Such an outcome would, for all intents and purposes, effectively grant immunity to these Defendants and all similarly situated health care providers who become subject to fraud allegations brought pursuant to the [FCA]."<sup>33</sup>

In support of its holding, the *Roberts* court cited a long line of cases where courts rejected application of state peer review privileges in federal antitrust and employment discrimination matters for similar reasons.<sup>34</sup>

---

28 *Id.* (quoting *Mem'l Hosp. for McHenry Cty.*, at 1061).

29 *Id.* (quoting *Mem'l Hosp. for McHenry Cty.*, at 1061–62).

30 *Id.*

31 *Id.* The FCA (since the major 1986 amendments) does not require "actual knowledge," but instead defines knowledge to include reckless disregard and deliberate ignorance. 31 U.S.C. § 3729(b)(1).

32 *Id.*

33 *Id.*

34 *Id.* (citing various other cases that rejected application of the peer review privilege including *Mem'l Hosp. for McHenry Cty.*, at 1062 (restraint of trade case), *Holland v. Muscatine Gen. Hosp.*, 971 F. Supp. 385 (S.D. Iowa 1997) (Title VII case), and *Price v. Howard Cty. Gen. Hosp.*, 950 F. Supp. 141, 144 n.3 (D. Md. 1996) (antitrust matter)).

According to the *Roberts* court, these matters were different from medical malpractice cases, where peer review comments are not relevant to that critical issue (i.e., the care employed by the treating physician), and plaintiffs can prove their cases using other evidence.<sup>35</sup> The court noted that although the defendant doctor's degree of care would certainly be an issue, "the gravamen of the Relators' case focuses on the intentional and knowing actions taken by the Defendants to defraud the federal government," and the evidence of that mens rea, if it existed, would only be found in the peer review materials.<sup>36</sup> The court therefore concluded that Indiana's peer review statute was inconsistent with federal common law and should not apply.<sup>37</sup>

In contrast to *Roberts*, which follows the general rule against applying a state peer review privilege to preclude discovery of materials in a federal False Claims action, a rare exception is *Elkharwily v. Mayo Holding Company*.<sup>38</sup> There were, however, several unique factors present in *Elkharwily* that supported the court's application of the state peer review privilege. First, *Elkharwily* was an employment dispute brought under various state and federal statutes, including the FCA's anti-retaliation provision, and there were no substantive FCA claims in the plaintiff's complaint.<sup>39</sup> The plaintiff sought certain documents related to mortality conferences in discovery that the defendant claimed were protected by Minnesota's peer review privilege.<sup>40</sup> The magistrate judge reviewed these documents *in camera* and denied the plaintiff's motion to compel discovery based, in part, on the peer review privilege.<sup>41</sup>

---

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.* See also *United States v. United Network for Organ Sharing*, No. 02 C 2295 (N.D. Ill. May 17, 2002) (concluding OIG subpoena was within OIG's authority, was not too indefinite, and the information sought was reasonably relevant, rejecting defendant's arguments related to the peer review privilege).

<sup>38</sup> *Elkharwily v. Mayo Holding Co.*, No. 12-3062 (D. Minn. July 21, 2014).

<sup>39</sup> *Id.*

<sup>40</sup> *Id.*

<sup>41</sup> *Id.*

Upon the plaintiff's objection to the magistrate judge's ruling, the district court first noted it could modify or set aside the magistrate judge's order only "if it [was] clearly erroneous or contrary to law."<sup>42</sup> The court held that because the plaintiff brought claims under both state and federal law, it was "within the court's discretion to apply the state peer review privilege statute," and that it was not "clearly erroneous" for the magistrate judge to conclude that the state statute applied.<sup>43</sup> Finally, the court noted that the magistrate judge did not issue a blanket ruling applying the privilege to the case, "but instead ordered that once the privilege logs are exchanged, and an evaluation can be made as to whether the peer review privilege applies as to specific documents, then any unresolved issues can be brought to the court on motion for a determination."<sup>44</sup> The court held that this approach, which included *in camera* inspection, "balances the interests of encouraging effective review of medical care and disclosure of documents and information which have a close degree of relevance to a hospital's knowledge and investigation of the conduct of physicians in violation of federal law."<sup>45</sup>

The court's decision in *Elkharwily* should not be viewed as a full victory for an FCA defendant. The presence of very particular factors in the case might explain its deviation from the nearly universal rule that state peer review privilege does not apply in federal FCA matters: specifically in *Elkharwily*, the only FCA claim was one for retaliation; the plaintiff brought both state and federal claims; the magistrate judge did not issue a blanket ruling but permitted objections after exchanges of privilege logs; and the district court could sustain the plaintiff's objections only if the magistrate judge's order was clearly erroneous.<sup>46</sup> As a result, health

---

42 *Id.*

43 *Id.*

44 *Id.* (internal citations and alterations omitted).

45 *Id.* (internal quotation marks and citations omitted).

46 It remains an open question whether state peer review privileges might apply to *state* False Claims Act matters, an issue that appears to be completely unaddressed by any court.

care providers and their counsel wanting to protect self-critical material from discovery in FCA actions must look elsewhere for protection.

### Application of the federal self-critical analysis privilege

Given the failure of courts to extend state peer review privileges to materials sought in relation to FCA investigations, as well as distinctions between both the purpose and method of peer review proceedings and compliance audits, health care providers seeking a solution might next consider the potential application of the federal self-critical analysis privilege; however, the federal self-critical analysis privilege offers little if any protection to health care providers and counsel seeking to limit the discoverability of self-critical analysis.

Although there is no federal peer review privilege, many federal courts do recognize a self-critical analysis privilege. As described by one district court:

The self-critical analysis privilege has been recognized as a qualified privilege which protects from discovery certain critical self-appraisals. It allows individuals and businesses to candidly assess their compliance with regulatory and legal requirements without creating evidence that may be used against them by their opponents in future litigation. The rationale for the doctrine is that such critical self-evaluation fosters the compelling public interest in observance of the law.<sup>47</sup>

The self-critical analysis privilege appears to have first been recognized in 1970 by a federal court in *Bredice v. Doctors Hospital*, where the district court for the District of Columbia in a medical malpractice suit held that committee minutes concerning the death of the decedent, created “with the purpose of self-improvement,” were “entitled to a qualified

---

47 *Reichhold Chems. v. Textron*, 157 F.R.D. 522, 524 (N.D. Fla. 1994) [hereinafter *Reichhold Chems.*].

privilege on the basis of [ ] overwhelming public interest.”<sup>48</sup> Since then, the self-critical analysis privilege has been extended beyond the medical peer review context to protect other types of audits, including equal employment practices, accounting records, securities law, accident investigations, product safety assessments, and products liability.<sup>49</sup>

In subsequent years, federal courts have often applied a multi-part test in determining whether the self-critical analysis privilege applies. For the privilege to apply, (i) the information must have resulted from a self-critical analysis performed by the party seeking protection; (ii) there must be a strong public interest in preserving the free flow of the type of information sought; (iii) the information must be of the type such that its flow would be curtailed if discovery were allowed; and (iv) the document(s) in question must have been prepared with the expectation of confidentiality.<sup>50</sup>

As they have been in relation to applying state peer review privileges, however, federal courts have been reluctant to apply the self-critical analysis privilege to FCA matters. For example, in *United States ex rel. Falsetti v. Southern Bell*, the relators brought an FCA suit against a telephone company alleging the defendant knowingly billed the federal government for telephone access lines it knew were out of service.<sup>51</sup> Before the court was relators’ motion to compel the production of documents relating to certain internal investigations and audits.<sup>52</sup> The defendant objected to production of such documents based upon, among other things, the self-critical analysis privilege.<sup>53</sup>

---

48 *Bredice v. Doctors Hosp., Inc.*, 50 F.R.D. 249, 251 (D.D.C. 1970), *aff’d without opin.*, 479 F.2d 920 (1973).

49 *Reichhold Chems.*, 157 F.R.D. at 525 (collecting various cases).

50 *United States ex rel. Sanders v. Allison Engine Co., Inc.*, 196 F.R.D. 310, 312 (S.D. Ohio 2000). (citing *Hickman v. Whirlpool Corp.*, 186 F.R.D. 362, 363 (N.D. Ohio 1999) [hereinafter *Allison Engine Co.*]).

51 *United States ex rel. Falsetti v. S. Bell Tel.*, 915 F. Supp. 308, 309 (N.D. Fla. 1996) (Sherrill, Mag. J.).

52 *Id.*

53 *Id.*

After reviewing the history of the privilege, the court found that the privilege was inconsistent with the FCA.<sup>54</sup> Specifically, the *Falsetti* court focused on the FCA's reduced damages provision.<sup>55</sup> Under that provision, the court is limited to assessing double damages where a person or entity fully cooperates with the government in its investigation and voluntarily discloses an FCA violation within 30 days without any knowledge of a governmental investigation and prior to any action being commenced.<sup>56</sup> The court described this provision as creating "a safe-haven for persons who uncover past violations and act promptly to disclose the same to Government investigators."<sup>57</sup> According to the court, the reduced damages provision was important because it meant that Congress had "already considered the competing interests," and "provided its own version of a self-critical analysis privilege."<sup>58</sup> Accordingly, the court concluded that the general self-critical analysis privilege could not be applied to an FCA qui tam.<sup>59</sup>

The district court in *United States ex rel. Sanders v. Allison Engine Company* also rejected application of the self-critical analysis privilege to an FCA qui tam, noting that *even if* the privilege applied, the defendant would not be permitted to protect everything contained in the documents in question, as the privilege "applies only to analysis or evaluation, not the facts on which evaluation is based."<sup>60</sup> In *Allison Engine*, the relators filed a motion to compel the defendant's production of documents that related to certain internal audits.<sup>61</sup> The defendant argued the documents were protected from discovery under the self-critical analysis privilege.<sup>62</sup> The

---

54 *Id.* at 312–13.

55 *Id.* at 312.

56 *Id.* (citing reduced damages provision, currently found at 31 U.S.C. § 3729(a)(2)).

57 *Id.* The court also noted that the FCA offers a further incentive for voluntary disclosure by making any information disclosed pursuant to any such voluntary disclosure FOIA-exempt. *Id.* (citing what is now codified at 31 U.S.C. § 3729(c)).

58 *Id.* at 313.

59 *Id.*

60 *Allison Engine Co.*, at 315.

61 *Id.* at 311.

62 *Id.*

court stated that even if the privilege existed (it discussed multiple general criticisms of the privilege at length), “the justifications for it do not support its application to voluntary, routine reviews.”<sup>63</sup> The court applied the four-factor test discussed above and found that several of the factors did not support application of the privilege.<sup>64</sup> As to the second factor (the public must have a strong interest in preserving the free flow of the type of information sought), the court noted that although the public did have an interest in companies “continually trying to improve their production and efficiency . . . there is also a strong public interest in having government contractors meet their contractual obligations.”<sup>65</sup> The court in *Allison Engine* pointed out that other courts had uniformly “refused to apply the privilege where the documents in question have been sought by a governmental agency.”<sup>66</sup>

The court also concluded that the third factor (the information must be of the type whose flow would be curtailed if discovery were allowed) was “a close case.”<sup>67</sup> The court gave two reasons for why it doubted a company would stop engaging in self-critical analysis for fear the information might later be discoverable: First, ceasing internal review and improvement processes would be harmful for business.<sup>68</sup> Second, the documentation might actually form an affirmative defense to a claim, thereby making companies more inclined to perform the self-critical analysis to protect themselves in the event of litigation.<sup>69</sup> Finally, the court held that the defendant failed to meet the fourth factor (the privilege protects only those documents that were prepared with the expectation

---

63 *Id.* at 313.

64 *Id.* at 312–13.

65 *Id.* at 314.

66 *Id.* The court did not address how this conclusion might be affected by the fact that the litigation before it was brought by a private whistleblower on the government’s behalf, and not the government itself.

67 *Id.*

68 *Id.*

69 *Id.*

of confidentiality) because another company was permitted to request those documents at any time.<sup>70</sup>

Although it is possible that a future court faced with a very specific set of facts might be willing to extend the federal self-critical analysis privilege to the FCA context, that possibility is remote if existing case law is any indication. Accordingly, health care providers must seek other protections to lower the risk that self-critical material is discoverable and can be used against them in subsequent investigations or litigation. The remainder of this article will discuss the use of attorney-client privilege to accomplish this goal.<sup>71</sup>

## Using Attorney-Client Privilege to Protect Self-Critical Material

In today's climate, which emphasizes the importance of audits and yet, state peer review privileges and the federal self-incrimination privilege are not likely to apply to protect the findings of those audits from subsequent governmental investigations, attorneys must focus on the protections afforded by the attorney-client privilege. Generally, the attorney-client privilege protects communications relating to a client seeking legal advice from an attorney;<sup>72</sup> however, the attorney-client privilege has frequently been extended to protect information and documents created by individuals inside the company in the course of an internal review or investigation, as well as work created by outside consultants as

---

70 *Id.* at 314–15.

71 Although the author was not able to find a case on point, an FCA defendant could possibly prevent certain self-critical material from being admitted into evidence under Federal Rule of Evidence 407, Subsequent Remedial Measures: If a health care provider discovered an instance of incorrect coding and took steps to correct future errors, the provider might argue that this evidence of a subsequent remedial measure cannot be introduced into evidence for the purpose of proving liability. This would be a fact-specific inquiry, however, and would not prevent the government from obtaining the information during investigation.

72 *In re OM Grp. Sec. Litig.*, 226 F.R.D. 579, 587 (N.D. Ohio 2005).



long as the work is created for the purpose of assisting the attorney in providing legal advice.

For example, in *In re OM Securities Litigation*, the plaintiffs sought to compel the defendants to produce documents created by an outside forensic accounting firm hired by defendants' outside counsel.<sup>73</sup> The documents in question were created as part of an internal investigation and consisted of notes regarding presentations and meetings with the audit committee prepared by either outside counsel or the outside accounting firm; spreadsheets, memoranda, and notes prepared by the outside accounting firm; and emails between or among the outside counsel, the accounting firm, and defendants' employees.<sup>74</sup> The court noted that "[t]he attorney-client privilege extends to memoranda and working papers prepared by an accountant at an attorney's request to assist the attorney in giving legal advice to the client."<sup>75</sup> After reviewing the relevant documents in question, the court concluded that the documents listed above were protected by the attorney-client privilege because they were prepared "in order to enable [the outside law firm] to give legal advice to the Audit Committee."<sup>76</sup>

This privilege has been recognized in the FCA context. In *United States ex rel. Robinson v. Northrop Grumman Corporation*, the relators sought documents created by Arthur Young & Company (AY), an independent auditor that was hired for purposes of an internal investigation.<sup>77</sup> According to the defendant, the investigation was undertaken by its internal legal department "in anticipation of a wide-scale government audit as a way to gauge [its] regulatory compliance and potential liability."<sup>78</sup> The relators disagreed with the defendant's privilege assertion and moved

---

73 *Id.* at 583–84.

74 *Id.* at 588–89.

75 *Id.* at 588–89.

76 *Id.* at 589. The court did go on to find that the defendants waived the attorney-client privilege in part by disclosing certain information. *Id.* at 593–94.

77 *United States ex rel. Robinson v. Northrop Grumman Corp.*, No. 89 C 6111 (N.D. Ill. Nov. 5, 2002) (Mason, Mag. J.).

78 *Id.*

to compel.<sup>79</sup> While several non-attorneys from the defendant were involved in the investigation, an in-house attorney officially retained AY.<sup>80</sup> Although the relators did not disagree that, at least in theory, “an in-house attorney’s engagement of an outside auditor to help provide legal advice to a corporation may protect attorney-client privilege,” the relators argued that, in this particular case, the investigation was “funneled” through the legal department solely for the purpose of creating a privilege.<sup>81</sup>

The court in *Northrop* acknowledged that the initial idea of the internal investigation did not originate from in-house counsel’s office, and that counsel’s office was brought in after the idea was formulated and AY was first contacted, but concluded that this was not dispositive.<sup>82</sup> The court specifically noted that “[t]he engagement had not begun at the time the legal department became involved and it is not unusual for a project’s scope to change from the time of its original conception to its actual implementation.”<sup>83</sup> The court found that the legal department and in-house attorney contacted AY within days of the first contact by a non-attorney, and that there was no evidence that the defendant sought after-the-fact protection of potentially damaging material.<sup>84</sup>

After an *in camera* review, the court further concluded that the report created by AY as part of the investigation was protected by attorney-client privilege.<sup>85</sup> The court stated that the investigation “was conducted in order to provide [the in-house attorney] with the ability to give legal advice to Northrop[.]”<sup>86</sup> The court also found it compelling that certain

---

79 *Id.* The defendant also filed a motion for a protective order, seeking to have the relators return a particular privileged document related to the internal investigation that it inadvertently produced. *Id.*

80 *Id.*

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

85 *Id.*

86 *Id.*

conclusions from the defendant's first internal investigation were used to define the scope of a subsequent investigation, and that the relators had access to documents produced in relation to the subsequent investigation, which contained relevant factual information and conclusions "without delving into any legal analysis or information."<sup>87</sup>

Although both *OM Securities Litigation* and *Northrop* involved the use of outside consultants during the course of an internal investigation, the attorney-client privilege has been held to apply where the review is conducted internally without the use of outsiders. In fact, in its landmark decision in *Upjohn Company v. United States*, the Supreme Court held that where communications made during the course of an internal investigation were made by corporate employees to in-house counsel at the direction of corporate superiors in order to secure legal advice from counsel, those communications are privileged.<sup>88</sup> More recently, in *In re Kellogg Brown & Root*, a non-health care FCA matter from the D.C. Circuit, the relator sought discovery of documents related to an internal investigation conducted by the defendant Kellogg Brown & Root (KBR) into the alleged fraud that served as the basis for the FCA complaint.<sup>89</sup> The defendant claimed that the documents were protected by the attorney-client privilege because the internal investigation "had been conducted for the purpose of obtaining legal advice . . . ."<sup>90</sup> The district court reviewed the documents *in camera* and concluded that the documents were not privileged because the defendant had failed to dem-

---

87 *Id.*; see also *Davis v. City of Seattle*, No. C06-1659Z, at 2-4 (W.D. Wash. Nov. 20, 2007) (holding that attorney-client privilege protected communications between outside investigator and City Attorney's Office for purposes of securing legal advice for city); *Memry Corp. v. Ky. Oil Tech, N.V.*, No. C04-03843 RMW (HRL) (N.D. Cal. Jan. 4, 2007) (communications between advisor/agent and corporate counsel covered by privilege); *Motisola Malikha Abdallah v. Coca-Cola Co.*, No. 1:98-cv-3679-RWS (N.D. Ga. Jan. 25, 2000) (holding documents created by outside consultant privileged where company hired consultant for purpose of assisting in-house counsel in advising company regarding audit); *McCaugherty v. Siffermann*, 132 F.R.D. 234, 238-39 (N.D. Cal. 1990) (communications between advisor/agent and corporate counsel covered by privilege).

88 *Upjohn Co. v. United States*, 449 U.S. 383, 394-95 (1981) [hereinafter *Upjohn*].

89 *In re Kellogg Brown & Root, Inc.*, 756 F.3d 754, 756 (D.C. Cir. 2014).

90 *Id.*

onstrate that the communications “would not have been made ‘but for’ the fact that legal advice was not sought.”<sup>91</sup> Reversing the district court, the D.C. Circuit held that the defendant’s assertion of privilege was materially indistinguishable from the assertion in *Upjohn*.<sup>92</sup>

The D.C. Circuit in *KBR* rejected the district court’s distinction from *Upjohn* based on the fact that KBR’s investigation involved solely in-house counsel, not outside attorneys.<sup>93</sup> The circuit court noted the general rule that “a lawyer’s status as in-house counsel ‘does not dilute the privilege.’”<sup>94</sup> The circuit court also rejected the district court’s focus on non-attorneys conducting many of the interviews in KBR’s internal investigation,<sup>95</sup> noting that the investigation was conducted “at the direction of the attorneys” in KBR’s in-house legal department.<sup>96</sup> The circuit court held that “communications made by and to non-attorneys serving as agents of attorneys in internal investigations are routinely protected by the attorney-client privilege.”<sup>97</sup>

The circuit court in *KBR* also rejected the district court’s holding that, because KBR’s internal investigation was undertaken to comply with government regulations that required defense contractors to maintain a compliance program and conduct internal investigations, the investigation was not performed to obtain or provide legal advice.<sup>98</sup> The circuit court held that “[s]o long as obtaining or providing legal advice was *one of* the significant purposes of the internal investigation, the attorney privilege applies, even if there were also other purposes for the investigation and even if the investigation was mandated by regulation rather than simply an exercise of company discretion.”<sup>99</sup> The circuit court concluded that because “one of the significant purposes of the [KBR] internal

---

91 *Id.* (quoting district court’s decision).

92 *Id.* at 757 (citing *Upjohn*, at 389).

93 *Id.* at 758.

94 *Id.* (quoting *In re Sealed Cases*, 737 F.2d 94, 99 (D.C. Cir. 1984)).

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.*

99 *Id.* at 758–59 (emphasis added).

investigation was to obtain or provide legal advice[.]” the documents in question were protected by attorney-client privilege.<sup>100</sup>

Cases like *Upjohn* and *KBR* demonstrate the importance of counsel’s role in an internal audit or investigation to maintain privilege. It is important to note, however, that an attorney’s (in-house or outside counsel) involvement in an internal audit or investigation does *not* automatically mean the information created is privileged. For example, in *Resnick v. American Dental Association*, the plaintiff sued the American Dental Association (ADA) claiming discriminatory employment practices.<sup>101</sup> Before the court was a motion to compel the discovery of a study conducted by Booz Allen, an outside management firm hired by the defendant to perform a “personnel practices study.”<sup>102</sup> The defendant claimed that the study and related documents were protected by the attorney-client privilege because the study was undertaken “with the advice and assistance of counsel.”<sup>103</sup> After rejecting the defendant’s claims that the material was protected by the self-critical analysis privilege and the work product doctrine, the court addressed the defendant’s attorney-client privilege claim.<sup>104</sup> The court rejected this claim of privilege as well, noting that it was not enough that the work in question “was initiated with advice of counsel, and counsel for ADA was kept advised of the activities as they progressed.”<sup>105</sup> The court concluded that the attorney-client privilege did not apply because “the work was essentially management-oriented for ADA’s overall business purposes, so that the lawyer-client relationship was no more than tangential to the studies.”<sup>106</sup> As discussed above, the key factor is that the work is created for the purpose of assisting

---

100 *Id.* at 760.

101 *Resnick v. ADA*, 95 F.R.D. 372, 373 (N.D. Ill. 1982).

102 *Id.* at 374.

103 *Id.*

104 *Id.* at 374–76. As to the work product doctrine, the court rejected its application because the material in question was not “prepared in anticipation of litigation or for trial,” which is required for the doctrine to apply. *Id.* at 375.

105 *Id.*

106 *Id.*

counsel in providing legal advice.<sup>107</sup> Accordingly, providers and their legal counsel would be well-advised to clearly document work that is created for this privileged purpose and not for a non-privileged reason, such as purely business purposes.

Although attorney-client privilege could apply in situations where either in-house or outside counsel is utilized, the use of in-house counsel poses unique risks that might make the use of outside counsel to oversee and direct internal audits and reviews the more prudent choice. For example, in *United States v. ChevronTexaco Corporation*, the court discussed the complications of attorney-client privilege when in-house, as opposed to outside, counsel is involved:

[C]ommunications between a corporation and its outside counsel are presumed to be made for the purpose of seeking legal advice . . . unlike outside counsel, in-house attorneys can serve multiple functions in the corporation . . . . Accordingly, communications involving in-house counsel might well pertain to business rather than legal matters. The privilege does not protect an attorney's business advice. Corporations may not conduct their business affairs in private simply by staffing a transaction with attorneys. Because in-house counsel may operate in a purely or primarily business capacity in many corporate endeavors, the presumption that attaches to communications with outside counsel does not extend to communications with inside counsel.<sup>108</sup>

---

107 *In re OM Grp. Sec. Litig.*, 226 F.R.D. 579, 588 (N.D. Ohio 2005).

108 *United States v. ChevronTexaco Corp.*, 241 F. Supp. 2d 1065, 1076 (N.D. Cal. 2002) (emphasis in original) (internal citations omitted).

The court in *ChevronTexaco* held that the defendant was required to make a “clear showing” that the speaker made the communications with the “primary purpose” of securing legal advice.<sup>109</sup> Accordingly, while reviews directed by in-house counsel, such as those in *Northrop*, might be protected if it can be clearly shown that the primary purpose of the review is to help in-house counsel provide legal advice to the company, the *ChevronTexaco* analysis would seem to indicate this purpose will be presumed if the company utilizes outside counsel to direct the investigation.

In addition to ensuring that the self-critical material is developed with the purpose of securing legal advice, to ensure attorney-client privilege protection for an internal audit or investigation, the entity must maintain strict confidentiality. The Tenth Circuit stated that “[b]usiness confidentiality is key to the privilege . . . The courts will grant no greater protection to those who assert the privilege than their own precautions warrant.”<sup>110</sup> In this respect, it is prudent that all documents created during the course of the review are marked “confidential” or “privileged,” and segregated from other, non-privileged documents. In *Hardy v. New York News*, the court found that audit information undertaken by the company’s Equal Employment Opportunity manager was not protected by the attorney-client privilege where none of the documents were marked with these designations and where the documents in question were intermingled with other, non-privileged documents.<sup>111</sup> Accordingly, it is prudent for providers and their counsel to ensure that all self-critical analysis documents prepared at the direction of counsel are properly marked as such (e.g., “Prepared at direction of counsel, privileged and confidential”) and kept segregated from non-privileged material.

In summary, to ensure the strongest argument for privilege where outside consultants are utilized, best practices would recommend that outside counsel retain the consultant directly and make clear in a writ-

---

<sup>109</sup> *Id.*

<sup>110</sup> *In re Qwest Commc’ns. Int’l*, 450 F.3d 1179, 1185 (10th Cir. 2006).

<sup>111</sup> *Hardy v. N.Y. News Inc.*, 114 F.R.D. 633, 644 (S.D.N.Y. 1987).

ten engagement agreement that the consultant is being hired for the purpose of assisting counsel in providing legal advice, that the consultant is to work at the direction of counsel, and that any work intended to be performed is protected by applicable privileges, such as the attorney-client privilege and work product doctrine, where applicable.<sup>112</sup> Further, counsel should “closely oversee and direct the work of consultants.”<sup>113</sup> Where in-house counsel directs the investigation or review, it is even more important to be clear throughout the process that corporate counsel is acting in his or her role as legal counsel, and that the investigation is being conducted for the purpose of assisting counsel in providing legal advice to the company. Whether in-house or outside counsel are providing the advice, the materials must be kept confidential so that any applicable privilege is not waived.

## Conclusion

While health care providers are well advised to conduct regular and thorough internal audits and reviews to ensure continued compliance with ever-changing health care rules and regulations, they should take steps to protect self-critical material from subsequent investigations or litigation. Unfortunately, courts have consistently and almost universally rejected the application of state peer review privileges and the federal common law self-critical analysis privilege in FCA matters. Accordingly, health care providers must be careful and proactive about protecting compliance reviews from subsequent discovery by the government or an FCA relator. The best way to ensure protection and avoid subsequent disclosure is to structure internal audits and investigations

---

112 See STEVEN E. FAGELL ET AL., PRACTISING LAW INST., PRACTICAL GUIDANCE FOR MAINTAINING PRIVILEGE OVER AN INTERNAL INVESTIGATION 6–7 (2014), available at [https://www.cov.com/files/Publication/8bae79a5-a1da-41fd-9192-1ea6b6d86c62/Presentation/PublicationAttachment/5008c055-c877-49ab-b13c-28295017c9f2/PLI\\_CHB-Practical\\_Guidance\\_for\\_Maintaining\\_Privilege.pdf](https://www.cov.com/files/Publication/8bae79a5-a1da-41fd-9192-1ea6b6d86c62/Presentation/PublicationAttachment/5008c055-c877-49ab-b13c-28295017c9f2/PLI_CHB-Practical_Guidance_for_Maintaining_Privilege.pdf). This engagement letter should also expressly instruct the consultant to clearly mark all papers and communications “confidential” and “privileged.”

113 *Id.* at 7.



so that they are conducted at the direction of counsel and, therefore, protected by attorney-client privilege. One of the most important roles of a health care attorney is to give advice regarding whether a client is operating in compliance with the myriad rules and regulations governing health care. Conducting internal audits at the direction of counsel assists counsel in providing legal advice; if done properly, such audits can be conducted in a privileged fashion, but simply having an attorney involved is not enough to ensure that protection. The provider and the provider's counsel should be careful to ensure that all of the elements of the attorney-client privilege are met and maintained throughout the course of the review and thereafter.

## NOTES AND COMMENTS

### Five Years After *NFIB*: Is Medicaid Expansion Still Feasible?

Jeffery Rowe

**What is the issue?** As the Medicaid expansion envisioned by the Affordable Care Act remains optional for each state in the wake of the Supreme Court's decision in *National Federation of Independent Business v. Sebelius*, state lawmakers must evaluate the consequences of declining federal dollars at the risk of impacting uninsured residents, health care entities, and rural hospitals.

**What is at stake?** Since 2012, states have had the authority to decide whether to expand Medicaid. Health care policymakers and legislators in states that have not expanded their Medicaid programs should, therefore, examine the extent to which non-expansion is affecting health care needs and uncompensated care costs as compared to states that have expanded Medicaid.

**What should attorneys do?** Attorneys should keep abreast of growing evidence that Medicaid expansion improves access to care, strengthens the financial stability of safety-net health care providers, and positively impacts health care delivery systems—as well as the potential for state legislative changes that may impact health care clients' business opportunities.

**CITATION:** Jeffery Rowe, *Five Years After NFIB: Is Medicaid Expansion Still Feasible?*, J. HEALTH & LIFE SCI. L., Feb. 2017 at 36. © 2017 American Health Lawyers Association, [www.healthlawyers.org/journal](http://www.healthlawyers.org/journal). All rights reserved.

*Author biography appears on the next page.*

Jeffery Rowe is an Equal Access to Justice Scholar focusing on health care law at Mercer University School of Law (JD expected 2017). He is interested in assisting health care providers and nonprofit organizations in business, regulatory compliance, and public policy. Contact him via email at [prowe17@lawmail.mercer.edu](mailto:prowe17@lawmail.mercer.edu).

## Rowe: Is Medicaid Expansion Still Feasible?

### CONTENTS

Introduction .....	39
Background: Medicaid Expansion as an Enforcement Mechanism of the ACA.....	40
<i>National Federation of Independent Business v. Sebelius</i> and its Implications .....	42
Medicaid after <i>NFIB</i> : The coverage gap and opting out.....	43
Voluntary Medicaid Expansions Since <i>NFIB</i> .....	46
The Arkansas path in 2013 .....	47
The Pennsylvania path in 2015.....	50
The Louisiana path in 2016.....	52
Expanding Medicaid in the Remaining Non-Expansion States.....	53
Medicaid expansion: A good deal.....	54
What expanding Medicaid in non-expansion states would look like .....	59
Conclusion .....	65

## Introduction

Despite passage of the Patient Protection and Affordable Care Act (ACA) in 2010, roughly 2.6 million low-income Americans lack health insurance in 2016. They represent the “coverage gap” resulting from states’ decisions to not accept federal Medicaid dollars.<sup>1</sup> Ninety-one percent of this uninsured population resides in the South, with 56% residing in Florida, Georgia, and Texas.<sup>2</sup> Although some lawmakers have argued that the cost of expanding Medicaid is too expensive, health policy experts and medical professionals argue that failing to expand Medicaid results in a net loss of billions of dollars in federal funding, exacerbating dire hardships for residents and hospitals in non-expansion states.<sup>3</sup>

Residents and hospitals in non-expansion states will benefit if this Medicaid coverage gap is closed. Medicaid expansion in the remaining states will increase access to health care, promote job growth, and reduce the overall cost of care. This Note will explore how data from expansion states indicate that the influx of federal dollars has reduced hospital closures, generated an increase in local jobs, and contributed to state tax revenue.<sup>4</sup> Most critically, hundreds of thousands of Americans previously lacking access to health care now have much-needed health insurance.

This Note will proceed in four parts. [The background on Medicaid expansion under the ACA](#) will evaluate Medicaid’s growth and subsequent expansions, along with the ACA’s use of Medicaid as an enforcement mechanism to expand health care access. Next, this Note will analyze the turning point of and future implications for Medicaid with the

---

1 See RACHEL GARFIELD & ANTHONY DAMICO, KAISER COMM’N ON MEDICAID & THE UNINSURED, THE COVERAGE GAP: UNINSURED POOR ADULTS IN STATES THAT DO NOT EXPAND MEDICAID—AN UPDATE 1 (2016), available at <http://files.kff.org/attachment/Issue-Brief-The-Coverage-Gap-Uninsured-Poor-Adults-in-States-that-Do-Not-Expand-Medicaid>.

2 *Id.* at 2.

3 See, e.g., WILLIAM S. CUSTER, HEALTHCARE GA. FOUND., THE ECONOMIC IMPACT OF MEDICAID EXPANSION IN GEORGIA 4 (2013) [hereinafter THE ECONOMIC IMPACT OF MEDICAID EXPANSION IN GEORGIA], available at [www.healthcaregeorgia.org/uploads/file/Georgia\\_Medicaid\\_Economic\\_Impact.pdf](http://www.healthcaregeorgia.org/uploads/file/Georgia_Medicaid_Economic_Impact.pdf).

4 See, e.g., Jack Hoadley & Adam Searing, *The Ripple Effects of Medicaid Expansion*, HEALTH AFF. BLOG (Jun. 7, 2016), <http://healthaffairs.org/blog/2016/06/07/the-ripple-effects-of-medicaid-expansion/> (last visited Nov. 6, 2016).

Supreme Court's 2012 decision in *National Federation of Independent Business v. Sebelius* (*NFIB*), which rendered Medicaid expansion optional for each state. The section on [voluntary Medicaid expansion since \*NFIB\*](#) will discuss states that have reached political compromise to expand Medicaid, namely Arkansas, Pennsylvania, and Louisiana. Finally, the Note will apply the Arkansas, Pennsylvania, and Louisiana models to the remaining non-expansion states in an attempt to predict that [Medicaid expansion can be politically and economically feasible](#), if not inevitable.

## Background: Medicaid Expansion as an Enforcement Mechanism of the ACA

Congress has expanded the Medicaid program four times since its inception in 1965, leading up to the passage of the Affordable Care Act in 2010.<sup>5</sup> Seeking to address serious problems facing the nation's health care system, Congress extended eligibility for Medicaid coverage under the ACA to include citizens and legal residents with incomes up to 133% of the federal poverty level (FPL),<sup>6</sup> then standardizing income-eligibility for recipients in all categories based on a modified adjusted gross income by applying a 5% disregard, essentially raising the threshold to 138% FPL.<sup>7</sup>

Perhaps most significant, however, is that states may now offer an existing Medicaid benefit package or "benchmark-equivalent" coverage<sup>8</sup> to non-elderly, non-disabled single adults or couples without children, as well as all children, including those under age six.<sup>9</sup> Benchmark-

---

5 See *Medicaid Timeline*, KAISER FAMILY FOUND. (Mar. 24, 2015), <http://kff.org/medicaid/timeline/medicaid-timeline/> (last visited Nov. 6, 2016) (tracking the earlier Medicaid expansions in 1967, 1972, 1988, and 2003).

6 See generally Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119, § 2001(a)(1) (codified at 42 U.S.C. § 1396a(a)(10)(A)(i)(VIII)) [hereinafter *ACA*].

7 *Id.* (ACA income threshold was increased to 138% FPL through section 1004(e) of the Health Care and Education Reconciliation Act of 2010.).

8 *Id.* §§ 1302(a)(1), 2001(a)(2)(A), 1396a(k)(1), 1396u-7(b)(5) (mandating that states cover this category of beneficiaries providing at least the essential health benefits package).

9 See *id.* § 2001(a)(1)(c) (contrasting the pre-ACA requirement that children be within 100% FPL between ages 6 and 18).

equivalent coverage allows states to offer plans with benefits that include inpatient and outpatient hospital services, prescription drugs, mental health services,<sup>10</sup> and family-planning supplies and services.<sup>11</sup> These benchmark-equivalent benefits were designed to include the package of essential health benefits (EHB) required for private-individual and small-group plans; they also must have an aggregate actuarial value that is at least equivalent to the generally-available state employee plan.<sup>12</sup>

As of late 2016, children represent nearly 50% of all Medicaid beneficiaries, while the elderly and individuals with disabilities represent 24%. The remaining 26% are comprised primarily of non-elderly and non-disabled adults.<sup>13</sup> Prior to the ACA, income eligibility tests varied among category and states. Children up to age 5 were required to be covered up to 133% FPL, whereas children ages 6 to 18 only had a 100% FPL cap.<sup>14</sup> On the other hand, pregnant women were required to be covered up to 133% FPL, although some states chose to cover pregnant women at higher income levels.<sup>15</sup>

When a state opts into the Medicaid program, the state and the federal government enter into a “state plan” agreement setting forth which groups will be eligible for coverage and methodologies for provider

---

10 See Nicole Huberfeld et al., *Plunging into Endless Difficulties: Medicaid and Coercion in National Federation of Independent Business v. Sebelius*, 93 B.U. L. Rev. 1, 26 [hereinafter *Plunging into Endless Difficulties*] (observing that benchmark-equivalent coverage is less comprehensive than the traditional statutorily-defined benefits package).

11 ACA § 2303(c) (requiring coverage of family planning services, et al.).

12 See *id.* § 2001(c)(3) (requiring that benchmark-equivalent plans cover pre-defined EHB after 2014).

13 See *Distribution of Medicaid Enrollees by Enrollment Group, FY2011*, KFF.ORG, <http://kff.org/medicaid/state-indicator/distribution-of-medicaid-enrollees-by-enrollment-group/?currentTimeframe=0&sortModel=%7B%22colld%22:%22Location%22,%22sort%22:%22asc%22%7D> (last visited Nov. 6, 2016) (noting that children comprise 48% of enrollees nationwide for fiscal year 2011).

14 See Medicare Catastrophic Coverage Act of 1988 § 302, 42 U.S.C. § 1396a(a)(10)(A)(i) (establishing coverage for children between 6 and 19 years of age and up to 100% FPL).

15 See *id.* § 1396a(a)(10)(A)(i)(III)–(V) (mandating coverage for pregnant women at or below 133% FPL and up to 185% FPL at each state’s discretion).

reimbursement.<sup>16</sup> The Medicaid Act requires the provision of seven forms of medical services such as inpatient and outpatient hospital, nursing-facility, nurse-midwife, and nurse practitioner services.<sup>17</sup> Optional services such as dental care and prescription drug coverage are also available.<sup>18</sup> Under the Medicaid Act, a state may not deny services based solely on a beneficiary's diagnosis, illness, or condition<sup>19</sup> and beneficiaries are statutorily entitled to receive prompt services without waiting periods.<sup>20</sup> While states creating a state plan are required to meet certain federal standards, individual health care providers are not required to participate in the Medicaid program.<sup>21</sup> Rather, states are required to provide reimbursement that ensures provider participation with "equal access" to non-Medicaid patients within the geographic area.<sup>22</sup>

### ***National Federation of Independent Business v. Sebelius and its Implications***

In 2010, after Congress passed and President Obama signed the ACA into law, several opponents—26 states, 2 private plaintiffs, and the National Federation of Independent Business—filed lawsuits asserting that the ACA exceeded congressional authority under the Spending Clause.<sup>23</sup> Specifically, the plaintiffs argued that the ACA's requirement for states to expand Medicaid surpassed federal spending power, which

---

16 See generally *Medicaid State Plan Amendments*, MEDICAID.GOV, [www.medicaid.gov/state-resource-center/medicaid-state-plan-amendments/medicaid-state-plan-amendments.html](http://www.medicaid.gov/state-resource-center/medicaid-state-plan-amendments/medicaid-state-plan-amendments.html) (last visited Nov. 6, 2016).

17 See also 42 U.S.C. §§ 1396a(a)(10)(A)(i), (a)(1)–(5).

18 *Id.* §§ 1396a(a)(10)(A)(i)–(ii), 1396d(a) (listing 28 categories of medical assistance, but requiring states to cover at least 7).

19 See 42 C.F.R. § 440.230(c).

20 See 42 U.S.C. § 1396a(a)(8) (requiring that State Plans ensure coverage "with reasonable promptness to all eligible individuals").

21 *Id.* § 1396a(a)(30)(A).

22 *Id.*

23 *Nat'l Fed'n of Indep. Bus. v. Sebelius*, 132 S. Ct. 2566 (2012) [hereinafter *NFIB*]; see also *Plunging into Endless Difficulties*, at 2.



amounted to unconstitutional coercion.<sup>24</sup> On appeal, the Eleventh Circuit upheld the district court's ruling on the grounds that Medicaid expansion was not akin to coercion because states retained their option of participating.<sup>25</sup> The Supreme Court granted certiorari and decided the case on June 28, 2012.<sup>26</sup>

In *NFIB*, a majority of the Court upheld the ACA's individual mandate as a valid exercise of Congress' general power to tax and spend, arguably saving the entire law by enforcing one of the ACA's key mechanisms.<sup>27</sup> At the same time, however, Chief Justice Roberts' plurality opinion effectively limited Congress' power to expand Medicaid under the Spending Clause by allowing states the option to forego Medicaid expansion without suffering a loss to existing funding.<sup>28</sup>

### Medicaid after *NFIB*: The coverage gap and opting out

While the ACA survived the Court's decision in *NFIB*, it emerged wounded. With Medicaid expansion optional, 32 states and the District of Columbia have chosen to expand Medicaid, while 19 states have opted out.<sup>29</sup>

To better understand why the coverage gap exists, it is helpful to understand arguments for and against Medicaid expansion. On the one hand, proponents of expansion contend that expansion has increased access to health care for millions of beneficiaries and has allowed states to earn between \$7 and \$8 in federal funding for every \$1 it spends on

---

24 Florida v. HHS, 780 F.Supp.2d 1256, 1266 (N.D. Fla. 2011) (holding that the individual mandate was unconstitutional, but rejecting the States' challenge to Medicaid expansion).

25 Florida v. HHS, 648 F.3d 1235, 1267–68 (11th Cir. 2011).

26 See generally *NFIB*.

27 *Id.* at 2601.

28 *Id.* at 2608.

29 See *Status of State Action on the Medicaid Expansion Decision*, KFF.org, <http://kff.org/health-reform/state-indicator/state-activity-around-expanding-medicaid-under-the-affordable-care-act/> (last visited Nov. 6, 2016) (listing status by state with the most recent data as of Mar. 14, 2016).

expansion.<sup>30</sup> On the other hand, the chief arguments against expansion are cost and uncertainty. For example, many states face a budget deficit and state leaders cannot justify the added expense.<sup>31</sup> Opponents also are concerned that states will face hidden administrative costs associated with expansion.<sup>32</sup> In addition, many states remain uncertain that the federal government will be able to guarantee the proposed match rate through 2020, especially in light of the growing federal deficit.<sup>33</sup>

By allowing states to opt out of Medicaid expansion, the *NFIB* decision has created a coverage gap of individuals who earn more than that state's previously established Medicaid eligibility limit, but less than the threshold to receive the ACA's Marketplace premium tax credits, thus lacking access to affordable health insurance.<sup>34</sup>

As of January 2016, 10 of the 19 states opting out of Medicaid expansion are located in the South, where 91% of the nation's 2.6 million Americans lacking health insurance reside.<sup>35</sup> Specifically, roughly 26% reside in Texas, 18% reside in Florida, 12% reside in Georgia, and 8% reside in North Carolina.<sup>36</sup> Racial and ethnic minority groups are more

---

30 STAN DORN & MATTHEW BUETTGENS, ROBERT WOOD JOHNSON FOUND. & URBAN INST., *THE COST TO STATES OF NOT EXPANDING MEDICAID* (2016), available at [www.rwjf.org/content/dam/farm/reports/issue\\_briefs/2016/rwjf430767](http://www.rwjf.org/content/dam/farm/reports/issue_briefs/2016/rwjf430767) [hereinafter *THE COST OF NOT EXPANDING*].

31 See generally Maggie Lee, *State GOP Leaders Double Down Against Medicaid Expansion*, MACON TELEGRAPH, Feb. 16, 2014, available at <http://insurancenewsnet.com/oarticle/State-GOP-leaders-double-down-against-Medicaid-expansion-a-461894>.

32 NAT'L ASS'N of CMTY. HEALTH CTRS., *MEDICAID: TO EXPAND OR NOT? KEY ECONOMIC ARGUMENTS USED ON BOTH SIDES* (2013), available at [www.nhchc.org/wp-content/uploads/2013/01/nachc-medicaid-economics.pdf](http://www.nhchc.org/wp-content/uploads/2013/01/nachc-medicaid-economics.pdf).

33 *Id.* at 3.

34 *Id.*; see also Samantha Artiga et al., *The Impact of the Coverage Gap for Adults in States Not Expanding Medicaid by Race and Ethnicity*, KFF.ORG, available at <http://kff.org/disparities-policy/issue-brief/the-impact-of-the-coverage-gap-in-states-not-expanding-medicaid-by-race-and-ethnicity/> (last visited Nov. 7, 2016) (mapping the status of Medicaid expansion since Sep. 1, 2015).

35 See RACHEL GARFIELD & ANTHONY DAMICO, KAISER COMM'N ON MEDICAID & THE UNINSURED, *THE COVERAGE GAP: UNINSURED POOR ADULTS IN STATES THAT DO NOT EXPAND MEDICAID—AN UPDATE 1, 3* (2016), available at <http://files.kff.org/attachment/Issue-Brief-The-Coverage-Gap-Uninsured-Poor-Adults-in-States-that-Do-Not-Expand-Medicaid>.

36 *Id.*

likely to lack health insurance and live in low-income families than their white, non-Hispanic counterparts, thereby comprising a larger segment of the coverage gap population.<sup>37</sup> In addition, states with a higher African-American population such as in Texas, Florida, and Georgia account for a significantly higher rate of individuals falling into the coverage gap.<sup>38</sup>

Some states' Medicaid programs have eligibility requirements that are more restrictive than others.<sup>39</sup> For instance, to qualify for coverage in Georgia—a state that has the nation's third-highest uninsured population after Texas and Florida<sup>40</sup>—the elderly, blind, or disabled cannot earn more than 75% over FPL (\$11,770 for a single person or \$15,930 for a family of two), and pregnant women may not earn more than 225% FPL (\$26,500 for single person or \$45,200 for a family of three).<sup>41</sup> Compared to the national average uninsured rate—10% in 2014<sup>42</sup>—roughly 16% of Georgians remain uninsured, generally either because those within a state's coverage gap exceed the state's Medicaid cutoff or they earn too little to qualify for subsidies through the federal health insurance marketplace.<sup>43</sup>

---

37 *Id.*

38 *Id.* (noting that the characteristics of the coverage gap vary depending on a state's population).

39 See, e.g., GA. BUDGET & POL'Y INST., UNDERSTANDING MEDICAID IN GEORGIA AND THE OPPORTUNITY TO IMPROVE IT (2015), available at <https://gbpi.org/wp-content/uploads/2015/09/Georgia-Medicaid-Chart-Book.pdf> [hereinafter UNDERSTANDING MEDICAID].

40 See Misty Williams, *The Red State Solution on Medicaid: Georgia's Not Part of It*, KAISER HEALTH NEWS, Apr. 1, 2015.

41 See UNDERSTANDING MEDICAID, at 5.

42 See *Health Insurance Coverage of the Total Population*, KFF.ORG, available at <http://kff.org/other/state-indicator/total-population/?currentTimeframe=0&sortModel=%7B%22coll%22:%22Location%22,%22sort%22:%22asc%22%7D> (last visited Nov. 7, 2016) (noting the disparity in health insurance coverage by state).

43 See UNDERSTANDING MEDICAID, at 10.

## Voluntary Medicaid Expansions Since *NFIB*

As of late 2016, states that voluntarily expanded Medicaid have thus far reported positive economic results in the form of budget savings, revenue gains, and overall economic growth.<sup>44</sup> States participating in Medicaid expansion, such as New Mexico, Colorado, Kentucky, Arkansas, and Alaska are projected to enjoy positive economic growth through 2021.<sup>45</sup> Other studies have concluded that expansion has benefited residents by reducing the number of unpaid bills and the amount of debt sent to third-party collection agencies.<sup>46</sup>

For states that chose not to expand their Medicaid programs, data has shown slower enrollment growth and providers have experienced little or no decline in uninsured visits and uncompensated care.<sup>47</sup> Health policy experts predict that the 19 non-expansion states would see federal subsidies in health insurance marketplaces fall by over \$129 billion, and reductions in uncompensated care could save up to \$27 billion while lowering federal spending by up to \$43 billion over the next decade if these states chose to expand Medicaid.<sup>48</sup>

States that have adopted Medicaid expansion cite a “moral imperative” for providing health coverage to low-income individuals, especially when the federal government offers billions of dollars to do so.<sup>49</sup> Arkansas and Louisiana—two states that are generally viewed as politically conservative—set themselves apart when they chose to expand their

---

44 LARISA ANTONISSE ET AL., KAISER COMM’N ON MEDICAID AND THE UNINSURED, THE EFFECTS OF MEDICAID EXPANSION UNDER THE ACA: FINDINGS FROM A LITERATURE REVIEW (2016), available at <http://files.kff.org/attachment/Issue-brief-The-Effects-of-Medicaid-Expansion-under-the-ACA-Findings-from-a-Literature-Review>.

45 *Id.* at 8.

46 *Id.* at 5 (noting that such cost savings occur in areas with high shares of low-income and uninsured residents).

47 *Id.* at 1.

48 See THE COST OF NOT EXPANDING, at 1.

49 See Julian Polaris, *The Unintended Uninsured: The Affordable Care Act’s Coverage Gap*, HARV. L. & POL’Y REV., <http://harvardlpr.com/2016/03/29/the-unintended-uninsured-the-affordable-care-acts-coverage-gap/> (last visited Nov. 13, 2016).

states' Medicaid programs.<sup>50</sup> As discussed in the sections that follow, Arkansas, Pennsylvania, and Louisiana serve as illustrative models on which states that have not expanded Medicaid can do so.

### The Arkansas path in 2013

Since Medicaid expansion began in Arkansas on January 1, 2014, the state has seen the sharpest decline of the uninsured rate in the country, dropping by nearly 13.5% during the first year.<sup>51</sup> This remarkable event perhaps seemed unlikely considering the political landscape in 2013.<sup>52</sup> Then-Democratic Governor Mike Beebe worked with the Republican-controlled legislature to create a bipartisan compromise: the “private option.”<sup>53</sup> Under the private option, Arkansas received a federal waiver to use Medicaid funds to purchase private health plans for newly eligible beneficiaries, rather than placing beneficiaries on the existing Medicaid program.<sup>54</sup> The Section 1115 waiver, granted by the Centers for Medicare and Medicaid Services (CMS), allows states to implement the ACA's Medicaid expansion using Medicaid dollars as premium assistance to purchase private Qualified Health Plans (QHP) on the Arkansas Mar-

---

50 See generally *Current Status of State Medicaid Expansion Decisions*, KFF.ORG, <http://kff.org/health-reform/slide/current-status-of-the-medicaid-expansion-decision/> (last visited Nov. 13, 2016).

51 See Dan Witters, *In U.S., Uninsured Rates Continue to Drop in Most States*, GALLUP, [www.gallup.com/poll/184514/uninsured-rates-continue-drop-states.aspx](http://www.gallup.com/poll/184514/uninsured-rates-continue-drop-states.aspx) (last visited Nov. 11, 2016) (indicating that the statewide uninsured rate was 22.5% in 2013 dropping to 9.1% in early 2015).

52 See JANE B. WISNER ET AL., ROBERT WOOD JOHNSON FOUND. & URBAN INST., MEDICAID EXPANSION, THE PRIVATE OPTION, AND PERSONAL RESPONSIBILITY REQUIREMENTS: THE USE OF SECTION 1115 WAIVERS TO IMPLEMENT MEDICAID EXPANSION UNDER THE ACA 5 (2015), available at [www.urban.org/sites/default/files/alfresco/publication-pdfs/2000235-Medicaid-Expansion-The-Private-Option-and-Personal-Responsibility-Requirements.pdf](http://www.urban.org/sites/default/files/alfresco/publication-pdfs/2000235-Medicaid-Expansion-The-Private-Option-and-Personal-Responsibility-Requirements.pdf) [hereinafter PERSONAL RESPONSIBILITY REQUIREMENTS].

53 See David Ramsey, *Governor Seeks New Concessions From CMS to Maintain Arkansas' Medicaid Expansion*, KAISER HEALTH NEWS, <http://khn.org/news/governor-seeks-new-concessions-from-cms-to-maintain-arkansas-medicaid-expansion/> (last visited Nov. 12, 2016) [hereinafter *New Concessions*].

54 *Id.*

ketplace.<sup>55</sup> Other states have also opted to expand Medicaid using the private option, covering newly eligible adults up to 138% FPL and requiring beneficiaries to make monthly income-based co-payments from \$5 to \$25 per month.<sup>56</sup> Such a compromise was politically palatable to Arkansas Republicans because the expansion mechanism was built upon politically conservative policies including privatization, wellness and work programs, and cost-sharing.<sup>57</sup> Thus, rather than expand Medicaid as originally envisioned by the ACA, the Arkansas plan extended insurance coverage to newly eligible beneficiaries by promoting private enterprise and fostering competition for marketplace coverage.<sup>58</sup>

Prior to adopting the private option, Arkansas—a state with nearly 3 million residents—had one of the nation’s narrowest Medicaid eligibility requirements, with nearly 20% of adults uninsured.<sup>59</sup> Since implementing the private option, both enrollees and hospitals have benefitted: Almost half of all enrollees now have health insurance for the first time in their lives, while hospitals have seen a 55% decrease in uncompensated care cost, with patients seeking care in community-based settings rather than emergency rooms.<sup>60</sup> In addition, the private option has increased competition on the Arkansas Marketplace and driven down the cost of Marketplace premiums. Enrollment of private insurers in

---

55 See *Medicaid Expansion in Arkansas*, KFF.ORG, <http://kff.org/medicaid/fact-sheet/medicaid-expansion-in-arkansas/> (last visited Nov. 12, 2016) (stating that Arkansas was the first state to use the Section 1115 waiver).

56 See *id.* (Iowa and New Hampshire also sought the private option via Section 1115 waivers as of Feb. 2015.).

57 See *New Concessions* (Indiana, Michigan, and Montana have negotiated waivers).

58 See PERSONAL RESPONSIBILITY REQUIREMENTS, at 6.

59 See *id.* (indicating that nearly 250,000 adults fell below the state’s Medicaid cutoff).

60 See JOCELYN GUYER ET AL., KAISER COMM’N ON MEDICAID & THE UNINSURED, A LOOK AT THE PRIVATE OPTION IN ARKANSAS (2015), available at <http://files.kff.org/attachment/issue-brief-a-look-at-the-private-option-in-arkansas> [hereinafter A LOOK AT THE PRIVATE OPTION IN ARKANSAS]; see also DEBORAH BACHRACH ET AL., ROBERT WOOD JOHNSON FOUND., THE IMPACT OF MEDICAID EXPANSION ON UNCOMPENSATED CARE COSTS: EARLY RESULTS AND POLICY IMPLICATIONS FOR STATES 1 (2016), available at [www.rwjf.org/content/dam/farm/reports/issue\\_briefs/2015/rwjf420741](http://www.rwjf.org/content/dam/farm/reports/issue_briefs/2015/rwjf420741) (defining uncompensated care costs as “generated in situations where hospitals and other providers deliver services to patients for which they are not fully compensated [...] because patients are uninsured or underinsured and unable to pay out of pocket for their services”).

the state-run Marketplace has nearly tripled from 2014 to 2016, while simultaneously creating a younger, healthier risk pool, resulting in a 2% drop in the average Marketplace premiums from 2014 to 2015.<sup>61</sup> Finally, Arkansas saved \$15.2 million in spending related to pregnant women in 2015, which the state projects to increase to \$24.4 million in 2016.<sup>62</sup>

Until late April 2016, the future of Arkansas' successful Medicaid program remained uncertain because the waiver was due to expire on December 31, 2016.<sup>63</sup> Arkansas elected a Republican governor in 2014, Asa Hutchinson, who supported continuing the private option but called for the creation of a task force to determine the future of the program into 2017 and beyond.<sup>64</sup> In March 2016, lawmakers endorsed Governor Hutchinson's private option plan, to be renamed "Arkansas Works," but remain divided over his proposal for managed care firms to administer services for developmentally disabled and mentally ill individuals.<sup>65</sup> Experts estimate ending Arkansas' Medicaid expansion would cost the state over \$400 million between 2017 and 2021, while costing hospitals roughly \$1 billion in uncompensated care costs during the same time period.<sup>66</sup> Governor Hutchinson recently vetoed the sunset provision of the Medicaid budget that ordered an end to the program on December 31, 2016, and Republican lawmakers were unable to override the veto, thus securing the future of Arkansas Works for the foreseeable future.<sup>67</sup>

---

61 See A LOOK AT THE PRIVATE OPTION IN ARKANSAS, at 1.

62 See DEBORAH BACHRACH ET AL., ROBERT WOOD JOHNSON FOUND., STATES EXPANDING MEDICAID SEE SIGNIFICANT BUDGET SAVINGS AND REVENUE GAINS 3 (2016) [hereinafter STATES EXPANDING MEDICAID] (representing a 50% decrease in spending during 2015).

63 See *New Concessions* (A 75% majority is needed in both chambers to continue expansion).

64 See PERSONAL RESPONSIBILITY REQUIREMENTS, at 8.

65 See *Arkansas Panel Backs Medicaid Plan, Split Over Managed Care*, ASSOCIATED PRESS, Mar. 7, 2016, available at [www.thv11.com/news/local/arkansas-panel-backs-medicaid-plan-split-over-managed-care/72617373](http://www.thv11.com/news/local/arkansas-panel-backs-medicaid-plan-split-over-managed-care/72617373).

66 See *New Concessions*.

67 See *Medicaid Expansion Plan Survives Veto Override Attempt*, ARK. NEWS, Apr. 26, 2016, [www.arkansasnews.com/news/arkansas/medicaid-expansion-plan-survives-veto-override-attempt](http://www.arkansasnews.com/news/arkansas/medicaid-expansion-plan-survives-veto-override-attempt) (last visited Nov. 12, 2016).

As of December 2016, Arkansas' Section 1115 waiver has been approved by CMS, which was the only remaining obstacle to implementing the changes called for under Arkansas Works.<sup>68</sup> Pursuant to CMS's approval of Arkansas Works, the 100% federal match will continue through the end of the year, and will drop to 90% by 2020.<sup>69</sup> Although CMS approved the state's request to incentivize businesses to provide employer-sponsored insurance, CMS restricted this to new employers offering insurance for the first time.<sup>70</sup>

### The Pennsylvania path in 2015

In late August 2014, CMS approved Pennsylvania's proposal for a Section 1115 waiver to expand Medicaid pursuant to the ACA under then Republican Governor Tom Corbett.<sup>71</sup> Under Governor Corbett's plan, dubbed "Healthy PA," to extend health care benefits to nearly 600,000 uninsured Pennsylvanians beginning on January 1, 2015, private companies would charge certain beneficiaries monthly premiums.<sup>72</sup> In contrast to Arkansas Works, Healthy PA calls for newly eligible 19 and 20-year-olds to be covered under Medicaid managed care.<sup>73</sup> The theory behind Pennsylvania's alternative expansion model was that citizens would

---

68 *State Waivers List*, MEDICAID.GOV, [www.medicaid.gov/medicaid/section-1115-demo/demonstration-and-waiver-list/waivers\\_faceted.html](http://www.medicaid.gov/medicaid/section-1115-demo/demonstration-and-waiver-list/waivers_faceted.html) (last visited Dec. 13, 2016).

69 See Virgil Dickinson, *Future of Arkansas' Medicaid Expansion Unclear as Lawmakers Start Special Session*, MODERN HEALTHCARE, Apr. 4, 2016, [www.modernhealthcare.com/article/20160404/NEWS/160409958](http://www.modernhealthcare.com/article/20160404/NEWS/160409958) (last visited Dec. 13, 2016).

70 See John Lyon, *Hutchinson: Feds OK Arkansas Works With Changes*, TIMES RECORD, Dec. 8, 2016, [www.swtimes.com/news/20161208/hutchinson-feds-ok-arkansas-works-with-changes](http://www.swtimes.com/news/20161208/hutchinson-feds-ok-arkansas-works-with-changes) (last visited Dec. 13, 2016).

71 See KAISER COMM'N ON MEDICAID & THE UNINSURED, MEDICAID EXPANSION IN PENNSYLVANIA: TRANSITION FROM WAIVER TO TRADITIONAL COVERAGE (2015) available at <http://kff.org/medicaid/fact-sheet/medicaid-expansion-in-pennsylvania/> [hereinafter MEDICAID EXPANSION IN PENNSYLVANIA].

72 *Id.*

73 See KAISER COMM'N ON MEDICAID & THE UNINSURED, MEDICAID EXPANSION THROUGH PREMIUM ASSISTANCE: ARKANSAS, IOWA, AND PENNSYLVANIA'S PROPOSALS COMPARED (2014), available at <https://kaiser-familyfoundation.files.wordpress.com/2014/04/8463-04-medicaid-expansion-through-premium-assistance-arkansas-iowa-and-pennsylvania.pdf>.



actively invest in their own health and wellness through cost sharing, not unlike in Iowa. Both Iowa's and Pennsylvania's plans call for most currently and newly eligible, noninstitutionalized adults ages 18 and up to pay a copay for non-emergency use of the emergency room.<sup>74</sup> Governor Corbett's plan called for premiums for adults with incomes above 100% FPL, but capped at 2% of a beneficiary's household income.<sup>75</sup> Pennsylvania also sought to reward beneficiaries by offering reduced monthly premiums for individuals who engage in "healthy behaviors," such as receiving an annual physical or participating in job training or work-search programs.<sup>76</sup> Unlike then Governor Beebe's private option model in Arkansas, however, Governor Corbett's Pennsylvania model created three benefits packages that grouped individuals into risk pools with similarly situated beneficiaries.<sup>77</sup>

Governor Corbett lost his reelection bid to Democrat Tom Wolf during the 2014 midterm elections. The newly inaugurated Governor Wolf announced in February 2015 his intentions to transition from the tiered alternative expansion plan to full Medicaid expansion as envisioned by the ACA through a state plan amendment (SPA).<sup>78</sup> Governor Wolf criticized his predecessor's plan as too complex and a hindrance to enrollment.<sup>79</sup>

---

74 *Id.* at 4.

75 See Amy Worden, *Feds Approve Corbett's Pa. Medicaid Expansion Proposal*, PHILLY.COM, [www.philly.com/philly/health/healthcare-exchange/20140829\\_Feds\\_approve\\_Corbett\\_s\\_Pa\\_Medicaid\\_expansion\\_proposal.html](http://www.philly.com/philly/health/healthcare-exchange/20140829_Feds_approve_Corbett_s_Pa_Medicaid_expansion_proposal.html) (last visited Dec. 14, 2016).

76 *Id.*

77 See MEDICAID EXPANSION IN PENNSYLVANIA, at 2 (Packages include a "high risk" package, a "low risk" package, and a managed care plan for otherwise healthy adults.).

78 See *Where the States Stand on Medicaid Expansion*, ADVISORY BOARD (Jan. 13, 2016), [www.advisory.com/daily-briefing/resources/primers/medicaidmap](http://www.advisory.com/daily-briefing/resources/primers/medicaidmap) (last visited Nov. 12, 2016).

79 See Mary K. Caffrey, *Pennsylvania Completes Switch to Traditional Medicaid Expansion*, AJMC.COM, Sep. 4, 2015, [www.ajmc.com/focus-of-the-week/0915/pennsylvania-completes-switch-to-traditional-medicaid-expansion](http://www.ajmc.com/focus-of-the-week/0915/pennsylvania-completes-switch-to-traditional-medicaid-expansion) (last visited Nov. 12, 2016) [hereinafter *Pennsylvania Completes Switch to Traditional Medicaid Expansion*].

Under Governor Wolf's plan, "HealthChoices," the three benefits packages created under Healthy PA were replaced with one benefit package and the monthly premiums and healthy behaviors program vanished.<sup>80</sup> As of September 2015, 440,000 enrollees have taken advantage of Medicaid expansion, and an additional 216,000 newly eligible Pennsylvanians enrolled since the beginning of the transition.<sup>81</sup> Consequently, Pennsylvania's uninsured population dropped from nearly 14% in 2015 to approximately 7% in May 2016.<sup>82</sup> The Pennsylvania Human Services Secretary estimates that the state has saved at least \$500 million in one year alone due to assistance from the federal government.<sup>83</sup>

### The Louisiana path in 2016

Louisiana, a state with 4.67 million residents,<sup>84</sup> became the thirty-second state to implement the ACA's Medicaid expansion when Governor John Bel Edwards signed an executive order the day after taking office in January 2016.<sup>85</sup> Unlike Arkansas and other states where the legislature must approve Medicaid expansion, health care policy decisions fall within the Louisiana governor's purview to act unilaterally, allowing him to bypass the state legislature.<sup>86</sup> The governor's decision to expand Medicaid in Louisiana would allow approximately 298,000 residents to

---

80 See MEDICAID EXPANSION IN PENNSYLVANIA, at 2.

81 See *Pennsylvania Completes Switch to Traditional Medicaid Expansion*.

82 See Elana Gordon, *One Year In, Pennsylvania Medicaid Expansion Prompts Celebration and Outreach*, NEWSWORKS, May 2, 2016, [www.newsworks.org/index.php/local/healthscience/93285-one-year-in-pennsylvania-medicaid-expansion-prompts-celebration-and-new-outreach](http://www.newsworks.org/index.php/local/healthscience/93285-one-year-in-pennsylvania-medicaid-expansion-prompts-celebration-and-new-outreach) (last visited Nov. 12, 2016).

83 *Id.*

84 See *Demographics and Census Geography: Louisiana State Census Data Center*, LOUISIANA.GOV, [http://louisiana.gov/Explore/Demographics\\_and\\_Geography/](http://louisiana.gov/Explore/Demographics_and_Geography/) (last visited Nov. 12, 2016).

85 See Richard Fausset & Abby Goodnough, *Louisiana's New Governor Signs an Order to Expand Medicaid*, N.Y. TIMES, Jan. 12, 2016, at A9, available at [www.nytimes.com/2016/01/13/us/louisianas-new-governor-signs-an-order-to-expand-medicaid.html?\\_r=0](http://www.nytimes.com/2016/01/13/us/louisianas-new-governor-signs-an-order-to-expand-medicaid.html?_r=0).

86 *Id.*

access health care and extend eligibility to an additional 224,000 privately insured adults.<sup>87</sup>

Louisiana's Medicaid expansion took effect on July 1, 2016. No data measuring the impacts yet exist, but experts remain hopeful.<sup>88</sup> Expanding Medicaid is expected to benefit both individuals and “safety net” hospitals providing critical access care. For example, the high cost of treating uninsured patients forced Baton Rouge General Medical Center to close its Mid City emergency room, an outcome that may have been avoided had Louisiana expanded Medicaid sooner.<sup>89</sup> Some practitioners remain concerned that Medicaid expansion could produce mixed results: specifically, new beneficiaries may have trouble finding doctors who accept Medicaid.<sup>90</sup> Many counter, however, that because 20% of Louisianans live in poverty, expanding Medicaid will offer an important opportunity to improve access to health care.<sup>91</sup>

## Expanding Medicaid in the Remaining Non-Expansion States

The chief arguments among opponents of Medicaid expansion in the remaining states are cost and uncertainty;<sup>92</sup> however, states may grapple with other valid economic issues. For instance, some have argued that

---

87 *Id.*

88 See KAISER COMM'N ON MEDICAID & THE UNINSURED, WHERE ARE STATES TODAY? MEDICAID AND CHIP ELIGIBILITY LEVELS FOR ADULTS, CHILDREN, AND PREGNANT WOMEN (2016), available at <http://kff.org/medicaid/fact-sheet/where-are-states-today-medicaid-and-chip/>.

89 See *Medicaid Expansion in Louisiana Could Produce Mixed Results*, BUS. REPORT, Feb. 12, 2016, [www.businessreport.com/article/medicaid-expansion-louisiana-produce-mixed-results](http://www.businessreport.com/article/medicaid-expansion-louisiana-produce-mixed-results) (last visited Nov. 12, 2016).

90 *Id.* (explaining that Medicaid reimbursements only cover roughly sixty-five cents on the dollar, limiting the number of physicians and providers who choose to treat Medicaid patients).

91 See Richard Fausset & Abby Goodnough, *Louisiana's New Governor Signs an Order to Expand Medicaid*, N.Y. TIMES, Jan. 12, 2016, at A9, available at [www.nytimes.com/2016/01/13/us/louisianas-new-governor-signs-an-order-to-expand-medicaid.html?\\_r=0](http://www.nytimes.com/2016/01/13/us/louisianas-new-governor-signs-an-order-to-expand-medicaid.html?_r=0).

92 See Maggie Lee, *State GOP Leaders Double Down Against Medicaid Expansion*, MACON TELEGRAPH, Feb. 16, 2014 [hereinafter *State GOP Leaders Double Down*].

the additional state and federal taxation can create a negative drag on local and state economies because personal income and business profits may be reduced.<sup>93</sup> Some opponents argue that any potential job growth in the health care industry created by Medicaid expansion could further contribute to unsustainable health care spending.<sup>94</sup>

Arkansas, Pennsylvania, and Louisiana demonstrate, however, that expanding Medicaid is not only politically and economically feasible, but doing so would likely increase state revenue and decrease uncompensated care costs. As recently as December 2015, Virginia<sup>95</sup> and Alabama<sup>96</sup> have pushed for Medicaid expansion despite political opposition. Although some governors and lawmakers generally remain opposed to Medicaid expansion,<sup>97</sup> low-income residents and hospitals alike would benefit from unlocking billions in federal dollars to develop state-specific solutions.

### Medicaid expansion: A good deal

The most common reason offered by non-expansion states for declining federal funds to expand Medicaid is cost: the state cannot afford to

---

93 EDMUND F. HAISLMAIER & DREW GONSHOROWSKI, HERITAGE FOUND., ISSUE BRIEF: STATE LAWMAKER'S GUIDE TO EVALUATING MEDICAID EXPANSION PROJECTS 3 (2012).

94 See Margot Sanger-Katz, *Health Care: Great for the Economy Today, Terrible Later*, NAT'L J., Feb. 2, 2013, available at [www.yahoo.com/news/health-care-great-economy-today-terrible-later-085520153--politics.html?ref=gs](http://www.yahoo.com/news/health-care-great-economy-today-terrible-later-085520153--politics.html?ref=gs).

95 See Editorial, *No Budging by Virginia Republicans on Medicaid Expansion*, WASH. POST, Dec. 19, 2015, available at [www.washingtonpost.com/opinions/no-budging-by-virginia-republicans-on-medicaid-expansion/2015/12/19/c7dfa1e4-a536-11e5-b53d-972e2751f433\\_story.html](http://www.washingtonpost.com/opinions/no-budging-by-virginia-republicans-on-medicaid-expansion/2015/12/19/c7dfa1e4-a536-11e5-b53d-972e2751f433_story.html) (Virginia's Democratic governor proposed a plan blocked by Republican legislators.).

96 See Peter Sullivan, *Alabama Latest State 'Looking' at Medicaid Expansion*, HILL, Nov. 13, 2015, available at <http://thehill.com/policy/healthcare/260050-alabama-governor-looking-at-obamacare-medicaid-expansion> (Alabama's Republican governor is "concerned about the plight of the working poor" and doctors practicing in rural areas.).

97 See Jim Galloway, *Obamacare and Red-State Reality: First Signs of a Negotiated Truce*, AJC.COM, Nov. 21, 2015, available at [www.ajc.com/news/state--regional-govt--politics/newsmedleystory3145358/4gtwtgY71pcsaVvWnHNsZP/](http://www.ajc.com/news/state--regional-govt--politics/newsmedleystory3145358/4gtwtgY71pcsaVvWnHNsZP/) [hereinafter *Obamacare and Red-State Reality*].

expand an already over-stretched program.<sup>98</sup> In Florida, Governor Rick Scott remains opposed to Medicaid expansion despite lawmakers' proposal during the 2015 legislative session.<sup>99</sup> Georgia's Governor Nathan Deal has repeatedly said that implementing such a program would cost the state approximately \$4 billion over ten years.<sup>100</sup> Finally, Texas' Governor Greg Abbott has declined expansion under the ACA, despite the fact that nearly one in five residents lacked health insurance in 2014.<sup>101</sup> This oft-repeated argument that expansion would cost too much has been the chief argument of opposition states across the country.<sup>102</sup>

A growing number of Republican governors have supported expansion, however. Michigan, Ohio, and Indiana have expanded Medicaid.<sup>103</sup> Although newly-elected Governor Matt Bevin desires to reverse Medicaid expansion in Kentucky,<sup>104</sup> the state is expected to add 40,000 jobs and \$30 billion to the state's economy through 2021 as a result of Medicaid expansion.<sup>105</sup>

---

98 See Misty Williams, *Medicaid Expansion Critical, Hospitals and MDs Say*, MYAJC., Oct. 31, 2013, available at [www.myajc.com/news/news/medicaid-expansion-critical-hospitals-and-mds-say/nbdpp/](http://www.myajc.com/news/news/medicaid-expansion-critical-hospitals-and-mds-say/nbdpp/) [hereinafter *Medicaid Expansion Critical*].

99 See Louise Norris, *The Inevitable Expansion of the Medicaid Expansion*, Health Insurance.org, Feb. 10, 2016, available at [www.healthinsurance.org/blog/2016/02/10/the-inevitable-expansion-of-the-medicaid-expansion/](http://www.healthinsurance.org/blog/2016/02/10/the-inevitable-expansion-of-the-medicaid-expansion/) (noting that no expansion bills have been introduced during the 2016 legislative session).

100 *Medicaid Expansion Critical*; see also *State GOP Leaders Double Down*.

101 See BENJAMIN D. SOMMERS, COMMONWEALTH FUND, *MEDICAID EXPANSION IN TEXAS: WHAT'S AT STAKE?* 2 (2016), available at [www.commonwealthfund.org/~media/files/publications/issue-brief/2016/apr/1870\\_sommers\\_medicaid\\_expansion\\_texas\\_v2.pdf](http://www.commonwealthfund.org/~media/files/publications/issue-brief/2016/apr/1870_sommers_medicaid_expansion_texas_v2.pdf) [hereinafter *MEDICAID EXPANSION IN TEXAS*].

102 See generally Bobby Jindal, *Opinion, Gov. Bobby Jindal: Why I Opposed Medicaid Expansion*, NOLA.com, July 23, 2013, [www.nola.com/opinions/index.ssf/2013/07/gov\\_bobby\\_jindal\\_why\\_i\\_opposed.html](http://www.nola.com/opinions/index.ssf/2013/07/gov_bobby_jindal_why_i_opposed.html) (last visited Nov. 13, 2016) (stating in an op-ed column that Medicaid "could" cost Louisianans \$1.7 billion over the first ten years).

103 See Editorial, *Medicaid Expansion in Red States*, N.Y. TIMES, Mar. 16, 2015, at A18, available at [www.nytimes.com/2015/03/16/opinion/medicaid-expansion-in-red-states.html?\\_r=0](http://www.nytimes.com/2015/03/16/opinion/medicaid-expansion-in-red-states.html?_r=0).

104 See Ashley Lopez, *Kentucky's New Governor Could Roll Back Medicaid, Even as State Benefits*, NPR, Dec. 8, 2015, available at [www.npr.org/2015/12/08/458887771/plans-to-roll-back-medicaid-expansion-doesn-t-seem-to-worry-rural-kentuckians](http://www.npr.org/2015/12/08/458887771/plans-to-roll-back-medicaid-expansion-doesn-t-seem-to-worry-rural-kentuckians).

105 See Press Release, Gov. Steve Beshear, *KY's Medicaid Expansion: 40,000 Jobs, \$30B Economic Impact* (Feb. 12, 2015), <http://migration.kentucky.gov/Newsroom/governor/20150212expansion.htm> (last visited Nov. 13, 2016).

A majority of residents in both Texas and Florida, the two largest states that have yet to expand Medicaid, favor expansion in their respective states.<sup>106</sup> This is perhaps unsurprising due to the rising costs of health care nationally. Marketing research firm Nielsen recently surveyed general attitudes towards health care costs and quality in five populous states: Texas, California, Florida, New York, and Ohio. The survey data indicated that a majority of residents from New York, Ohio, and California approve the decision to expand Medicaid and residents of both Texas and Florida overwhelmingly favored expansion.<sup>107</sup> Specifically, 63% of Texans and 68% of Floridians favored expansion.<sup>108</sup>

In Texas, for example, just over 5 million residents—one in five people—lacked access to health insurance in 2014.<sup>109</sup> This is due in part to the state's restrictive Medicaid eligibility requirements. Namely, Medicaid is available only to Texans with disabilities below 75% FPL, i.e., individuals who earn less than \$9,000 annually.<sup>110</sup> Consequently, low-income Texans have greater difficulty paying for and obtaining health care.<sup>111</sup> Texas' decision not to expand Medicaid is emblematic of other non-expansion states: adults in these states generally have less coverage than their counterparts in expansion states.

Yet, even if the estimates of lawmakers opposed to Medicaid expansion are accurate, and expansion does cost billions of dollars over the next decade, health policy experts predict that failing to expand Medicaid will have significant economic consequences. For example, Georgia was projected to lose \$33.7 billion in federal funding, and hospitals

---

106 See Carrie Feibel, *Majority of Texans and Floridians Want Medicaid Expansion*, Survey Shows, Kaiser Health News, May 24, 2016, <http://khn.org/news/majority-of-texans-and-floridians-want-medicaid-expansion-survey-shows/> (last visited Nov. 13, 2016).

107 *Id.*

108 *Id.*

109 See MEDICAID EXPANSION IN TEXAS, at 2.

110 *Id.*

111 *Id.* at 3.

\$12.8 billion in reimbursements until 2022.<sup>112</sup> Experts suggest that the actual state cost to cover expansion hovers closer to \$2.5 billion over ten years, nearly half of the governor's purported price tag.<sup>113</sup> By contrast, Texas was projected to leave \$65 billion dollars in federal funds on the table if it did not expand Medicaid, almost double that of Georgia.<sup>114</sup>

Medicaid expansion in the remaining non-expansion states would not only increase federal funding to provide health insurance coverage to over 2.9 million low-income Americans,<sup>115</sup> it would also produce other benefits. For example, data from 11 expansion states suggest that non-expansion states would enjoy cascading financial benefits as a result of federal dollars stabilizing struggling and rural hospitals, as well as promote job growth.<sup>116</sup> Expansion states enjoyed a 26% reduction in uncompensated care costs in 2014, compared to only a 16% reduction in non-expansion states.<sup>117</sup> Maryland, for example, reduced uncompensated care costs to hospitals by over \$13.5 million in 2015 because hospitals treated fewer uninsured patients.<sup>118</sup> A recent study published by the Department of Health and Human Services (HHS) found that insurance premiums are about 7% lower in expansion states than in

---

112 See STAN DORN ET AL., ROBERT WOOD JOHNSON FOUND. & URBAN INST., WHAT IS THE RESULT OF STATES NOT EXPANDING MEDICAID? 1 (2014), available at [www.urban.org/sites/default/files/alfresco/publication-pdfs/413192-What-is-the-Result-of-States-Not-Expanding-Medicaid-.pdf](http://www.urban.org/sites/default/files/alfresco/publication-pdfs/413192-What-is-the-Result-of-States-Not-Expanding-Medicaid-.pdf) (explaining that for every \$1 a state invests in Medicaid, \$13.41 in federal funds flow into the state).

113 *Id.* at 3 (noting that Georgia's cost would be \$254 million annually from 2013-2022).

114 *Id.* at 1.

115 See RACHEL GARFIELD & ANTHONY DAMICO, KAISER COMM'N ON MEDICAID & THE UNINSURED, THE COVERAGE GAP: UNINSURED POOR ADULTS IN STATES THAT DO NOT EXPAND MEDICAID—AN UPDATE 1, 3 (2016), available at <http://files.kff.org/attachment/Issue-Brief-The-Coverage-Gap-Uninsured-Poor-Adults-in-States-that-Do-Not-Expand-Medicaid> (noting that 56% of the 2.9 million Americans in the coverage gap reside in Florida, Georgia, and Texas).

116 See DEBORAH BACHRACH ET AL., ROBERT WOOD JOHNSON FOUND., STATES EXPANDING MEDICAID SEE SIGNIFICANT BUDGET SAVINGS AND REVENUE GAINS 1, 6 (2016), available at [www.rwjf.org/content/dam/farm/reports/issue\\_briefs/2016/rwjf419097](http://www.rwjf.org/content/dam/farm/reports/issue_briefs/2016/rwjf419097) [hereinafter STATES EXPANDING MEDICAID].

117 *Id.* at 2 (noting that expanding Medicaid drove down uncompensated care nationally by \$7.4 billion in 2014).

118 *Id.* at 5.



non-expansion states.<sup>119</sup> HHS Secretary Sylvia Burwell used the study to reiterate that expansion is a win-win for states because expanding Medicaid contributes to lower costs for Americans purchasing private insurance in the marketplace exchanges while expanding coverage to more people.<sup>120</sup>

Rural hospitals in non-expansion states are nearly twice as likely to close.<sup>121</sup> Georgia, in particular, suffers from poor rural hospital health; five rural hospitals have closed in that state since 2010.<sup>122</sup> Even legislators opposing Medicaid expansion recognize rural health care is one of the state's most pressing issues.<sup>123</sup> Although rural hospitals are in greater danger of closing in non-expansion states than in expansion states, this remains a distinct and multilayered problem caused by a number of factors, including, but not limited to, the failure of the hospitals to adapt to emerging health care delivery systems and aging facilities.<sup>124</sup>

Finally, expansion states enjoyed 33% higher job growth as compared to non-expansion states in 2014.<sup>125</sup> Research from Georgia State University health policy experts suggest that Medicaid expansion would generate

---

119 See Margot Sanger-Katz, *How Expanding Medicaid Can Lower Insurance Premiums for All*, N.Y. TIMES, Aug. 25, 2016, [www.nytimes.com/2016/08/26/upshot/how-expanding-medicaid-may-lower-insurance-premiums.html](http://www.nytimes.com/2016/08/26/upshot/how-expanding-medicaid-may-lower-insurance-premiums.html) (last visited Nov. 13, 2016).

120 *Id.*

121 See STATES EXPANDING MEDICAID, at 2 (basing measurements on financial strength, population risk, and quality outcomes).

122 See Ayla Ellison, *A State-by-State Breakdown of 57 Rural Hospital Closures*, BECKER'S HOSP. CFO, Sept. 15, 2015, [www.beckershospitalreview.com/finance/a-state-by-state-breakdown-of-57-rural-hospital-closures.html](http://www.beckershospitalreview.com/finance/a-state-by-state-breakdown-of-57-rural-hospital-closures.html) (last visited Nov. 13, 2016); see also *Obamacare and Red-State Reality*.

123 See Andy Miller, *Suburban Lawmaker Champions Cause of Rural Hospitals in Georgia*, GA. HEALTH NEWS, Feb. 11, 2016, [www.georgiahealthnews.com/2016/02/suburban-lawmaker-champions-rural-hospitals/](http://www.georgiahealthnews.com/2016/02/suburban-lawmaker-champions-rural-hospitals/) (last visited Nov. 13, 2016).

124 See JANE WISNER ET AL., KAISER COMM'N ON MEDICAID & THE UNINSURED, A LOOK AT RURAL HOSPITAL CLOSURES AND IMPLICATIONS FOR ACCESS TO CARE: THREE CASE STUDIES, *available at* <http://files.kff.org/attachment/issue-brief-a-look-at-rural-hospital-closures-and-implications-for-access-to-care> (exploring recent rural hospital closures in Kansas, Kentucky, and South Carolina).

125 See STATES EXPANDING MEDICAID, at 2.



over 70,000 jobs in Georgia alone—adding \$8.2 billion to the state's economic output—and generate increased tax revenue around \$276.5 million annually.<sup>126</sup> Nationwide, Medicaid expansion would generate both health care-related jobs (for private hospitals, private practitioners, and home health care services) and jobs outside the health care sector (e.g., the real estate industry, food services industry, transportation).<sup>127</sup> Many states also are beginning to understand the unintended effect Medicaid expansion has on reducing recidivism, while reducing criminal justice spending and associated costs with health treatment during and after release from prison.<sup>128</sup>

### What expanding Medicaid in non-expansion states would look like

Assuming state lawmakers decide to expand Medicaid, the question then is what would expansion look like under the various approaches? Perhaps the most direct approach would be to expand Medicaid as envisioned by the ACA and administered directly through CMS. Under this traditional approach, which was chosen by all but seven expansion states, CMS would not distribute federal funding until all newly eligible adults up to 138% FPL are covered.<sup>129</sup> Full Medicaid expansion as envisioned

---

126 See WILLIAM S. CUSTER, HEALTHCARE GA. FOUND., THE ECONOMIC IMPACT OF MEDICAID EXPANSION IN GEORGIA 1, 4 (2013), available at [www.healthcaregeorgia.org/uploads/file/Georgia\\_Medicaid\\_Economic\\_Impact.pdf](http://www.healthcaregeorgia.org/uploads/file/Georgia_Medicaid_Economic_Impact.pdf).

127 *Id.* at 5 (noting that over half of the jobs created by Medicaid expansion would be in the health care industry).

128 See generally JOCELYN GUYER ET AL., ROBERT WOOD JOHNSON FOUND., MEDICAID EXPANSION AND CRIMINAL JUSTICE COSTS: PRE-EXPANSION STUDIES AND EMERGING PRACTICES POINT TOWARDS OPPORTUNITIES FOR STATES (2015), available at <http://statenetwork.org/wp-content/uploads/2015/11/State-Network-Manatt-Medicaid-Expansion-and-Criminal-Justice-Costs-November-2015.pdf> (noting that Ohio's expansion saved \$10.3 million to cover inmates' inpatient care in 2014).

129 See MARYBETH MUSUMECI & ROBIN RUDOWITZ KAISER COMM'N ON MEDICAID & THE UNINSURED, THE ACA AND MEDICAID EXPANSION WAIVERS, available at <http://files.kff.org/attachment/issue-brief-the-aca-and-medicaid-expansion-waivers> [hereinafter THE ACA AND MEDICAID].

by the ACA seems unlikely, however, given the political climate and multiple other factors that can complicate the path to full expansion.<sup>130</sup>

President-elect Donald Trump seems to join Congressional Republicans in two key goals: (i) repeal and replace the ACA, and (ii) install a Medicaid block grant.<sup>131</sup> Pending legislative changes, the President-elect has announced that he intends to nominate Representative Tom Price (R-GA) to succeed HHS Secretary Sylvia Burwell.<sup>132</sup> Representative Price, a vocal critic of the ACA since its inception,<sup>133</sup> would have the authority as Secretary to re-interpret existing Medicaid program requirements and draft new regulations and guidance.<sup>134</sup> The President-elect's pick to oversee CMS, Indiana health care consultant Seema Verma, may enjoy a unique position in shaping the future of Medicaid.<sup>135</sup> Verma worked closely with Governor Mike Pence (R-IN) to create Healthy Indiana Plan (or HIP 2.0), Indiana's Medicaid expansion program.<sup>136</sup>

A Medicaid block grant policy would theoretically allow states greater flexibility to run their Medicaid programs as they see fit by providing an annual federal allotment.<sup>137</sup> Health policy experts remain concerned,

---

130 *Id.*

131 See *Key Medicaid Questions Post-Election*, KFF.ORG, <http://kff.org/medicaid/fact-sheet/key-medicaid-questions-post-election/> (last visited Dec. 13, 2016) [hereinafter QUESTIONS POST-ELECTION].

132 See JULIE ROVNER, FIVE QUICK WAYS A NEW HHS SECRETARY COULD CHANGE THE COURSE OF HEALTH POLICY, KAISER HEALTH NEWS, available at <http://khn.org/news/five-quick-ways-a-new-hhs-secretary-could-change-the-course-of-health-policy/> [hereinafter NEW HHS SECRETARY].

133 See Robert Pear, *Tom Price, Obamacare Critic, Is Trump's Choice for Health Secretary*, N.Y. TIMES, Nov. 28, 2016, available at [www.nytimes.com/2016/11/28/us/politics/tom-price-secretary-health-and-human-services.html](http://www.nytimes.com/2016/11/28/us/politics/tom-price-secretary-health-and-human-services.html).

134 See NEW HHS SECRETARY, at 1.

135 See Jake Harper, *Trump's Pick to Run Medicare and Medicaid Has Red State Policy Chops*, KAISER HEALTH NEWS, available at <http://khn.org/news/trumps-pick-to-run-medicare-and-medicaid-has-red-state-policy-chops/> (last visited Dec. 13, 2016).

136 *Id.*

137 See Robert Pear, *Expect Medicaid to Change, But Not Shrink, Under Donald Trump*, N.Y. TIMES, Nov. 15, 2016, available at [www.nytimes.com/2016/11/16/us/politics/trump-medicaid-health-care.html](http://www.nytimes.com/2016/11/16/us/politics/trump-medicaid-health-care.html).

however, that this would eliminate guaranteed coverage for all eligible, and that reduced federal funding would shift cost and risk to beneficiaries and states.<sup>138</sup>

In the meantime, Kentucky remains a model for Medicaid expansion through CMS under existing rules. Kentucky has been one of the most successful states because its uninsured rate dropped from 16% in 2013 to 8% in 2014, representing one of the largest reductions in the country,<sup>139</sup> opening access to care to low-income adults.<sup>140</sup> Medicaid expansion has created new jobs and driven down the uncompensated care costs of hospitals.<sup>141</sup> Perhaps more importantly, 72% of Kentuckians favor keeping the state's Medicaid program as is, despite the current governor's desire to reduce coverage under a waiver program, similar to Arkansas and Indiana.

The second alternative to expanding Medicaid in the remaining non-expansion states would be by executive order of the governor, the route that Louisiana,<sup>142</sup> Kentucky, and West Virginia took to expand Medicaid.<sup>143</sup> In Georgia, a state that ranks among states with the most

---

138 See QUESTIONS POST-ELECTION, at 2.

139 SAMANTHA ARTIGA ET AL., KAISER COMM'N ON MEDICAID & THE UNINSURED, IMPLEMENTATION OF THE ACA IN KENTUCKY: LESSONS LEARNED TO DATE AND THE POTENTIAL EFFECTS OF FUTURE CHANGES (2016), available at <http://kff.org/health-reform/issue-brief/implementation-of-the-aca-in-kentucky-lessons-learned-to-date-and-the-potential-effects-of-future-changes/>.

140 See KAISER FAM. FOUND. COMM'N ON MEDICAID & THE UNINSURED, WHAT'S AT STAKE IN THE FUTURE OF THE KENTUCKY MEDICAID EXPANSION? 1 (2016), available at <http://kff.org/medicaid/fact-sheet/whats-at-stake-in-the-future-of-the-kentucky-medicaid-expansion/> (last visited Sep. 3, 2016) [hereinafter WHAT'S AT STAKE].

141 *Id.* at 4.

142 See Richard Fausset & Abby Goodnough, *Louisiana's New Governor Signs an Order to Expand Medicaid*, N.Y. TIMES, Jan. 12, 2016, at A9, available at [www.nytimes.com/2016/01/13/us/louisianas-new-governor-signs-an-order-to-expand-medicaid.html?\\_r=0](http://www.nytimes.com/2016/01/13/us/louisianas-new-governor-signs-an-order-to-expand-medicaid.html?_r=0).

143 See KAISER COMM'N ON MEDICAID & THE UNINSURED, AN OVERVIEW OF ACTIONS TAKEN BY STATE LAWMAKERS REGARDING THE MEDICAID EXPANSION (2015), available at <http://files.kff.org/attachment/fact-sheet-an-overview-of-actions-taken-by-state-lawmakers-regarding-the-medicaid-expansion> [hereinafter ACTIONS TAKEN BY STATE LAWMAKERS].

executive orders issued from 2009 through 2013,<sup>144</sup> this pathway to expansion nonetheless seems unlikely. Although Governor Deal was previously authorized to take such action,<sup>145</sup> H.B. 990 requires a majority vote from the legislature before expanding Medicaid through the ACA, which essentially bars any Georgia governor from acting unilaterally.<sup>146</sup>

While an executive order is one path to Medicaid expansion, this route is not without its potential challenges. For example, following Governor Beshear's executive order expanding Medicaid in Kentucky, a small group of private citizens filed suit against the Commonwealth challenging the legality of the Kentucky statute authorizing the Secretary of Health and Family Services to accept federal funding.<sup>147</sup> Ultimately, the court held that the Secretary was permitted to "take advantage of all federal funds that may be available for medical assistance . . . ."<sup>148</sup>

The third and perhaps most likely pathway to providing health coverage to roughly 2.9 million low-income Americans would be to follow in the footsteps of Arkansas and six other states: expand Medicaid using a Section 1115 waiver.<sup>149</sup> This process provides a greater deal of flexibility because the state can create a program unique to the state's needs.<sup>150</sup> Through the waiver, non-expansion state residents could purchase pri-

---

144 See Joy Wang, *The Case of the Missing Executive Orders: (A Lack of) Transparency in Georgia's Government*, SUNLIGHT FOUND., Aug. 6, 2014, <https://sunlightfoundation.com/2014/08/06/the-case-of-the-missing-executive-orders-a-lack-of-transparency-in-georgias-government/>.

145 See GA. CONST. art. III, § IX, ¶ VI(b) (governor can proclaim a "major catastrophe" where funds can be utilized for relief purposes).

146 See Misty Williams, *Georgia Governor Basically Kills Medicaid Expansion*, GOVERNING, Apr. 13, 2014, [www.governing.com/news/headlines/georgia-governor-basically-kills-medicaid-expansion.html](http://www.governing.com/news/headlines/georgia-governor-basically-kills-medicaid-expansion.html) (last visited Nov. 13, 2016).

147 See ACTIONS TAKEN BY STATE LAWMAKERS, at 6.

148 *Id.*

149 See Kaiser Comm'n on Medicaid & the Uninsured, *Current Status of State Medicaid Expansion Decisions*, <http://kff.org/health-reform/slide/current-status-of-the-medicaid-expansion-decision/> (last visited Dec. 13, 2016) (Iowa, Indiana, Michigan, Montana, New Hampshire, and Pennsylvania have waivers as of Oct. 14, 2016).

150 See Rachel Sachs, *Medicaid Expansion Through Section 1115 Waivers: Evaluating the Tradeoffs*, HEALTH AFF. BLOG (Mar. 15, 2016), <http://healthaffairs.org/blog/2016/03/15/medicaid-expansion-through-section-1115-waivers-evaluating-the-tradeoffs/>.

vate health insurance on the exchange while paying small amounts in monthly premiums.<sup>151</sup> This pathway would likely be attractive to more conservative-leaning lawmakers because it promotes the ideals of private enterprise and market competition.<sup>152</sup> In addition, this approach offers greater state independence because lawmakers may try Medicaid expansion for a limited period of time with a reconsideration period to follow.<sup>153</sup>

Under a Trump Administration, however, the new HHS Secretary could foreseeably require an eligible beneficiary to work as a condition for Medicaid coverage, something the current administration has not approved.<sup>154</sup> For example, HHS rejected New Hampshire's waiver request in November 2016 because it sought to impose a work requirement and stricter standards that beneficiaries provide proof of United States citizenship and in-state residency.<sup>155</sup> The incoming administration will have the ability to decide how stringent or lenient the criteria for Section 1115 waivers will be.

It appears that lawmakers who once opposed Medicaid expansion may be yielding to the realities of the state health care systems. For example, Georgia's Health and Human Services Chair, Sen. Renee Unterman (R-Buford), has been working with her Republican colleagues to start a dialogue to present a plan to Governor Deal that would expand access

---

151 *Id.*

152 See JANE B. WISNER ET AL., ROBERT WOOD JOHNSON FOUND. & URBAN INST., MEDICAID EXPANSION, THE PRIVATE OPTION, AND PERSONAL RESPONSIBILITY REQUIREMENTS: THE USE OF SECTION 1115 WAIVERS TO IMPLEMENT MEDICAID EXPANSION UNDER THE ACA 1, 6 (2015), available at [www.urban.org/sites/default/files/alfresco/publication-pdfs/2000235-Medicaid-Expansion-The-Private-Option-and-Personal-Responsibility-Requirements.pdf](http://www.urban.org/sites/default/files/alfresco/publication-pdfs/2000235-Medicaid-Expansion-The-Private-Option-and-Personal-Responsibility-Requirements.pdf).

153 See THE ACA AND MEDICAID, at 3 (noting that there is no deadline for states to consider waivers or modify the expansion).

154 See QUESTIONS POST-ELECTION, at 4.

155 See Robert Pear, *Expect Medicaid to Change, but Not Shrink, Under Donald Trump*, N.Y. TIMES, Nov. 15, 2016, available at <http://www.nytimes.com/2016/11/16/us/politics/trump-medicaid-health-care.html>.

to care to hundreds of thousands of Georgians.<sup>156</sup> In addition, Georgia's doctors on the 7,000-member Medical Association of Georgia have similarly urged the governor to use the Section 1115 waiver.<sup>157</sup> Further, Grady Memorial Hospital—one of the nation's largest public safety-net hospitals<sup>158</sup>—is leading a charge alongside rural hospitals and health care facilities in Georgia to pursue the Section 1115 waiver.<sup>159</sup> Although Governor Deal refers to this approach as an “experiment” rather than “expansion” he concedes that it offers the greatest flexibility necessary to cover more people.<sup>160</sup>

Similarly, in Florida, there are indications of increasing openness to Medicaid expansion, albeit due to an emerging public health threat: Zika. Throughout the spring and summer of 2016, Governor Scott suggested that pregnant women should contact their doctors if they have concerns about contracting the virus.<sup>161</sup> The Florida Health Alliance, a coalition of 109 organizations working to expand access to health care and close the coverage gap, continues to lobby lawmakers and criticize Governor Scott because 300,000 women lack affordable access to physicians.<sup>162</sup> Florida's path to expansion remains murky. Last summer, the

---

156 See Greg Blustein, *More Georgia Republicans Want to Expand Medicaid, But It Will Be Tough*, AJC.COM, Jun. 27, 2016, at 1, [www.myajc.com/news/state--regional-govt--politics/more-georgia-republicans-want-expand-medicare-but-will-tough/jcxR7QYjyHct-s5yYz62i0l/](http://www.myajc.com/news/state--regional-govt--politics/more-georgia-republicans-want-expand-medicare-but-will-tough/jcxR7QYjyHct-s5yYz62i0l/) (last visited Dec. 14, 2016).

157 See Misty Williams, *Medicaid Expansion Critical, Hospitals and MDs Say*, MYAJC., Oct. 31, 2013, <http://www.myajc.com/news/medicaid-expansion-critical-hospitals-and-mds-say/nbdpp/> (last visited Nov. 13, 2016).

158 See Phil Galewitz, *Economy Boosts Safety-Net Hospitals in States Not Expanding Medicaid*, WASH. POST, Mar. 1, 2015, [www.washingtonpost.com/business/economy/economy-boosts-safety-net-hospitals-in-states-not-expanding-medicare/2015/03/01/642e9d4a-c025-11e4-ad5c-3b8ce89f1b89\\_story.html](http://www.washingtonpost.com/business/economy/economy-boosts-safety-net-hospitals-in-states-not-expanding-medicare/2015/03/01/642e9d4a-c025-11e4-ad5c-3b8ce89f1b89_story.html) (last visited Nov. 13, 2016).

159 See Greg Blustein, *Nathan Deal on Medicaid Waiver: More Would be Insured, But it's Still Not an Expansion*, AJC.COM, May 8, 2015, <http://politics.blog.ajc.com/2015/05/08/nathan-deal-on-medicare-waiver-more-would-be-insured-but-its-still-not-an-expansion/> (last visited Nov. 13, 2016).

160 *Id.*

161 See Liz Freeman, *Group Targets Rick Scott on Medicaid Expansion and Zika*, NAPLES DAILY NEWS, Aug. 23, 2016, [www.naplesnews.com/story/news/health/2016/08/22/89121100/](http://www.naplesnews.com/story/news/health/2016/08/22/89121100/) (last visited Nov. 13, 2016).

162 *Id.*

Senate overwhelmingly supported an \$80 billion bill that would expand Medicaid to cover about 800,000 Floridians, but it was rejected by the state House.<sup>163</sup>

Finally, as recently as May 2016, the Republican-led legislature and GOP Governor Mary Fallin in Oklahoma proposed to expand Medicaid using a Section 1115 waiver, which would prevent hospitals and nursing homes from closing by unlocking federal dollars to expand coverage to 175,000 residents.<sup>164</sup> Oklahoma's hospitals were facing a \$1.3 billion shortfall, thereby prompting lawmakers to realize that accepting billions of dollars in federal money was necessary.<sup>165</sup> In a surprising turn of events, however, the legislature passed an eleventh hour budget bill that provided the necessary funds for Oklahoma's hospitals and nursing homes for the next year, while stopping short of expanding Medicaid.<sup>166</sup>

## Conclusion

Medicaid has historically been a program aimed at providing affordable health care to the neediest members of our society. While the ACA intended to build on prior iterations by creating a national benchmark covering all qualifying low-income Americans, the Supreme Court's *NFIB* decision allows states to decide whether to expand Medicaid coverage. Six years after the ACA became law, governors and legislators in 19 states have not taken advantage of the federal dollars they could receive should they decide to expand their Medicaid programs. Non-expansion

---

163 See Nick Madigan, *Health Care Expansion is Rejected in Florida*, N.Y. TIMES, Jun. 5, 2015, at A12, available at [www.nytimes.com/2015/06/06/us/health-care-expansion-is-rejected-in-florida.html](http://www.nytimes.com/2015/06/06/us/health-care-expansion-is-rejected-in-florida.html).

164 See Marissa Evans, *Oklahoma Considering Medicaid Expansion*, WASH. HEALTH POL'Y WEEK IN REV., May 16, 2016, [www.commonwealthfund.org/publications/newsletters/washington-health-policy-in-review/2016/may/may-23-2016/oklahoma-considering-medicaid-expansion](http://www.commonwealthfund.org/publications/newsletters/washington-health-policy-in-review/2016/may/may-23-2016/oklahoma-considering-medicaid-expansion) (last visited Nov. 13, 2016).

165 *Id.*

166 See Marissa Evans, *Oklahoma Medicaid Expansion on Hold After Budget Deal*, WASH. HEALTH POL'Y WEEK IN REV., Jun. 6, 2016, [www.commonwealthfund.org/publications/newsletters/washington-health-policy-in-review/2016/jun/june-6-2016/oklahoma-medicaid-expansion-on-hold-after-budget-deal](http://www.commonwealthfund.org/publications/newsletters/washington-health-policy-in-review/2016/jun/june-6-2016/oklahoma-medicaid-expansion-on-hold-after-budget-deal) (last visited Nov. 13, 2016).

states argue that the post-federal support cost is too burdensome. Data from expansion states indicate, however, that economic growth and revenue generation more than offsets any financial burden. The data also seems to suggest that non-expansion plays a role in hospital closures, furthers job loss, and limits access to care from millions of Americans. Attorneys should keep abreast of this growing evidence that Medicaid expansion improves access to care, strengthens the financial stability of safety-net health care providers, and positively impacts health care delivery systems, while tracking the potential for state legislative changes that may impact health care clients' business opportunities under new federal leadership.



## NOTES AND COMMENTS

### The Yates Memo and the Push for Individual Accountability

Jonathan S. Feld and Eric S. Klein

**What is the issue?** In September 2015, the U.S. Department of Justice announced the implementation of more aggressive enforcement policies for corporate and individual prosecution. This fundamental policy shift now requires corporations, including the health care provider community, to identify individual wrongdoers and turn over all relevant facts related to persons responsible for corporate misconduct.

**What is at stake?** Given the “all or nothing” standard for cooperation credit that the DOJ has set, the agency’s emphasis on identifying responsible individuals creates potential conflicts of interest with employees or contractors who may be reluctant to cooperate with the company. Further, health care providers now face an increasing number of questions about how they can tailor their health care audits and investigations to provide the level of completeness that the DOJ might deem satisfactory.

**What should attorneys do?** Attorneys should counsel their health care provider clients on the issue of securing separate counsel for employees; ensure that both the company and its employees understand the distinction between the company’s attorney-client privilege and a personal privilege; and counsel their clients on how to strengthen the company’s corporate compliance program.

**CITATION:** Jonathan S. Feld and Eric S. Klein, *The Yates Memo and the Push for Individual Accountability*, J. HEALTH & LIFE SCI. L., Feb. 2017 at 67. © 2017 American Health Lawyers Association, [www.healthlawyers.org/journal](http://www.healthlawyers.org/journal). All rights reserved.

*Author biographies appear on the next page.*

**Jonathan S. Feld** is a Member at Dykema and leader of the firm's Government Investigations and Corporate Compliance Team. His practice focuses on complex civil and criminal matters, including antitrust, health care, financial, and anti-bribery actions. Contact him via email at [jfeld@dykema.com](mailto:jfeld@dykema.com).

**Eric S. Klein** is a Member at Dykema where he devotes his practice to representing clients in the health care sector with respect to corporate and regulatory issues. He counsels corporate and health care clients on compliance and reimbursement issues, fraud and abuse matters, provider practice acquisitions, business transactions, licensure, and Medicare/Medicaid certification matters. Contact him via email at [eklein@dykema.com](mailto:eklein@dykema.com).

## **Feld and Klein: The Yates Memo and Individual Accountability**

### **CONTENTS**

Introduction .....	70
The DAG Memos.....	71
What the Yates Memo Says .....	75
Reaffirmations of the Yates Memo in May 2016.....	78
The Yates Memo and civil cases.....	79
The Reverberations of the Yates Memo for Health Care .....	80
Increased importance of <i>Upjohn</i> warnings to employees.....	81
Concerns regarding attorney-client privilege and work product protection .....	83
Impact on administrative actions .....	84
Increased importance of compliance programs .....	87
Conclusion .....	88

## Introduction

On September 9, 2015, Deputy Attorney General (DAG) Sally Quillian Yates issued a memorandum titled “Individual Accountability for Corporate Wrongdoing.” Although the U.S. Department of Justice (DOJ) has long enforced a policy of holding individuals and corporations criminally and civilly liable for corporate misconduct, the “Yates Memo” announced the implementation of more aggressive enforcement policies for corporate and individual prosecution. The Yates Memo applies to many industries but once again, the health care industry, which has long been an enforcement priority for the DOJ, will be affected by the advent of this policy.

The Yates memo was, in part, a response to criticism about the lack of individual prosecutions in the aftermath of the 2008 economic collapse. Indeed, that criticism is still prevalent.<sup>1</sup> One key feature of the Yates Memo is the disclosure of “all relevant facts relating to the individuals responsible for the misconduct”<sup>2</sup> before the DOJ will consider any credit for cooperation that may reduce the company’s civil or criminal penalties. As DAG Yates explained on November 16, 2015:

In the past, cooperation credit was a sliding scale of sorts and companies could still receive at least some credit for cooperation, even if they failed to fully disclose all facts about individuals. That’s changed now. As the policy makes clear, providing complete information about individuals’ involvement in wrongdoing is a threshold hurdle . . . .<sup>3</sup>

- 
- 1 See, e.g., Senator Elizabeth Warren, Senate Floor Speech (Feb. 3, 2016), *available at* [www.warren.senate.gov/files/documents/2016-2-3\\_Warren\\_Floor\\_Speech.pdf](http://www.warren.senate.gov/files/documents/2016-2-3_Warren_Floor_Speech.pdf).
  - 2 Memorandum from Sally Quillian Yates, Deputy Attorney Gen. to Assistant Attorney-Gens., Dirs., and All U.S. Attorneys (Sept. 9, 2015), *available at* [www.justice.gov/dag/file/769036/download](http://www.justice.gov/dag/file/769036/download) [hereinafter *Yates Memo*].
  - 3 Sally Q. Yates, Deputy Attorney Gen., Office of the Deputy Attorney Gen., Remarks at American Banking Association and American Bar Association Money Laundering Enforcement Conference (Nov. 16, 2015), *available at* [www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-american-banking-0](http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-american-banking-0).

The “cooperation credit” creates a complicated dynamic between health care companies and their employees that has serious implications for internal investigations and the decision on whether to disclose to the DOJ.

This Comment explores the likely ramifications of the Yates Memo for the health care industry with (i) [a brief history of previous DAG memoranda](#) to illustrate how the DOJ’s guidance on corporate investigations has evolved, especially with regard to the protection given to attorney-client privileged information developed during internal investigations; (ii) [an analysis of the elements set forth in the Yates Memo](#) and how the DOJ has interpreted the Yates Memo since its release in September 2015; and (iii) [a review of the impact that the Yates Memo will have on corporate compliance and internal investigations](#).

## The DAG Memos

Over the past 17 years, one of the key functions of the Office of the Deputy Attorney General has been to provide guidance on the DOJ’s policies for criminal corporate prosecutions. From the outset, attorney-client privilege has been integral to the scope of corporate cooperation and voluntary disclosures, which are key factors in corporate prosecution principles. A brief review of the evolution of the DAG policies is instructive.

In 1999, then-DAG Eric Holder set out the factors considered in charging a corporation for criminal misconduct, including, but not limited to, the nature and seriousness of the offense, the pervasiveness of wrongdoing within the corporation, and the corporation’s history of similar conduct.<sup>4</sup> The Holder Memo acknowledged that “[i]n gauging the extent of the corporation’s cooperation, the prosecutor may consider the corporation’s willingness to identify the culprits within the corporation, including senior executives, to make witnesses available, to disclose complete results of its internal investigation, and to waive the attorney-client and

---

4 Memorandum from the Deputy Attorney Gen. to All Component Heads and U.S. Attorneys (June 16, 1999).

work product privileges.”<sup>5</sup> It further noted that the DOJ does not “consider waiver of a corporation’s privileges an absolute requirement, and prosecutors should consider the willingness of a corporation to waive the privileges when necessary to provide timely and complete information as only one factor in evaluating the corporation’s cooperation.”<sup>6</sup> The Holder Memo also made clear that “[p]rosecution of a corporation is not a substitute for the prosecution of criminally culpable individuals within or without the corporation” and that the “imposition of individual criminal liability on individuals provides a strong deterrent against future corporate wrongdoing.”<sup>7</sup>

The principle that corporate prosecution did not insulate or preclude prosecution of responsible individuals continued in successive DAG memos. In 2003, after the Enron and WorldCom scandals, then-DAG Larry D. Thompson issued a revised set of principles that made the Holder Memo guidelines mandatory on federal prosecutors.<sup>8</sup> The Thompson Memo adopted much of the language from the Holder Memo regarding corporate cooperation and voluntary disclosure, including consideration of the waiver of the attorney-client privilege:

One factor the prosecutor may weigh in assessing the adequacy of a corporation’s cooperation is the completeness of its disclosure including, if necessary, a waiver of the attorney-client privilege and work product protections, both with respect to its internal investigation and with respect to communications between specific officers, directors, and employees and counsel.<sup>9</sup>

The emphasis placed on voluntary waiver of the attorney-client privilege and work product protection in both the Holder and Thompson

---

5 *Id.* at 5.

6 *Id.* at 6.

7 *Id.* at 2.

8 Memorandum from Larry D. Thompson, Deputy Attorney Gen. to Heads of Dep’t Components U.S. Attorneys (Jan. 20, 2003).

9 *Id.* at 7.

Memos was controversial. From the view of defense counsel, it forced a corporation to either abstain from waiving the privilege at the risk of being labeled uncooperative, or release otherwise privileged information in hopes of receiving corporate credit that would mitigate its criminal liability.

That dilemma remained until 2006 when then-DAG Paul McNulty responded to criticism surrounding the DOJ's position on attorney-client privilege and work product protections.<sup>10</sup> The McNulty Memo announced that "[w]aiver of attorney-client and work product protections is not a prerequisite to a finding that a company has cooperated in the government's investigation."<sup>11</sup> Nonetheless, the McNulty Memo noted that the "disclosure of privileged information may be critical in enabling the government to evaluate the accuracy and completeness of the company's voluntary disclosure."<sup>12</sup> A demonstration of a "legitimate need" for the information requested would be required for prosecutors to seek a waiver of the privilege. The McNulty Memo described two categories of information that prosecutors could request if a legitimate need existed: (i) "purely factual information, which may or may not be privileged, relating to the underlying misconduct" and (ii) "[o]nly if the purely factual information provides an incomplete basis to conduct a thorough investigation should prosecutors then request that the corporation provide attorney-client communications or non-factual attorney work product."<sup>13</sup>

While, from the industry's perspective, the McNulty Memo was an improvement from the highly criticized policies set forth in the Holder and Thompson Memos, it still garnered its fair share of criticism. Opponents took issue with the fact that the McNulty Memo retained a policy that allowed prosecutors to not only seek privilege waivers during an investigation, but also created an award for those companies that complied with waiver requests.

---

10 Memorandum from Paul J. McNulty, Deputy Attorney Gen. to Heads of Dep't Components U.S. Attorneys (Dec. 12, 2006).

11 *Id.* at 8.

12 *Id.*

13 *Id.* at 9-10.

In 2008, then-DAG Mark Filip articulated a revised position. He explained that waiver of the “attorney-client privilege and work product protections has never been a prerequisite under the Department’s prosecution guidelines for a corporation to be viewed as cooperative.”<sup>14</sup> The Filip Memo specifically stated that “while a corporation remains free to convey non-factual or ‘core’ attorney-client communications or work product—if and only if the corporation voluntarily chooses to do so—prosecutors should not ask for such waivers and are directed not to do so.”<sup>15</sup> Corporate cooperation would depend on the entity’s readiness to disclose relevant facts relating to the alleged criminal misconduct, rather than its willingness to surrender otherwise privileged information.<sup>16</sup>

Eight years later, the Yates Memo relies on the same basic principles in evaluating allegations of corporate misconduct, but it has renewed questions regarding the level of deference that the DOJ will give to the attorney-client privilege and work product doctrine when deciding cooperation credit. DAG Yates has said she does not want to change existing DOJ policy. In her May 2016 speech, she explained her position:

[T]here is nothing in the Individual Accountability Policy that requires companies to waive attorney-client privilege or in any way rolls back protections already in place. The policy specifically requires only that companies turn over all relevant non-privileged information. We’re asking for the facts. And we have always asked for the facts. The only difference now is that companies cannot—in the name of privilege or otherwise—pick and choose which facts to provide if they want credit for cooperation. But, of course, if there is a valid claim

---

14 Memorandum from Mark Filip, Deputy Attorney Gen. to Heads of Dep’t Components U.S. Attorneys, at 8 (Aug. 28, 2008).

15 *Id.* at 9.

16 *Id.* at 9-11.



of privilege as to a relevant fact, we expect that it will be brought to the prosecutor's attention.<sup>17</sup>

While the broader policies of corporate cooperation and individual accountability have existed throughout the various DAG memos, the characterization that the privilege has been “misused” is an important shift and has ratcheted up the potential for tension when a company seeks to make voluntary disclosures. How the new policies of the Yates Memo will actually play out remains to be seen.

## What the Yates Memo Says

The DOJ identified four reasons in the Yates Memo for strengthening its pursuit of individual corporate wrongdoing: (i) deterring future illegal activity; (ii) incentivizing change in corporate behavior; (iii) ensuring that proper parties are held accountable for their actions; and (iv) promoting the public's confidence in the justice system. This rationale is not new—rather, it affirms well established DOJ objectives. As discussed [later](#), what it does is signal a much greater emphasis on meaningful corporate compliance programs and voluntary disclosures.

The Yates Memo identified six directives to federal prosecutors regarding the enhanced focus on individual prosecutions:

1. To be eligible for any cooperation credit, corporations must provide the DOJ with all relevant facts relating to the individuals responsible for the misconduct.
2. Criminal and civil corporate investigations should focus on individuals from the inception of the investigation.
3. Civil and criminal attorneys handling corporate investigations should be in routine communication with one another.

---

17 Press Release, Deputy Attorney Gen. Sally Q. Yates Delivers Remarks at the New York City Bar Association White Collar Crime Conference (May 10, 2016), [available at www.justice.gov/opa/speech/deputy-attorney-general-sally-q-yates-delivers-remarks-new-york-city-bar-association](http://www.justice.gov/opa/speech/deputy-attorney-general-sally-q-yates-delivers-remarks-new-york-city-bar-association) [hereinafter *May 2016 Speech*].

4. Absent extraordinary circumstances or approved DOJ policy, the DOJ will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation.
5. DOJ attorneys should not resolve matters with a corporation without a clear plan to resolve related individual cases.
6. Civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.<sup>18</sup> This sixth factor will be especially important to the health care sector because of the growth in civil False Claims Act matters, both by the government and whistleblowers.

The day after issuing the Yates Memo, DAG Yates delivered a speech on the DOJ's new policy where she described the DOJ's fundamental policy shift to requiring corporations to turn over all relevant facts related to individuals responsible for the misconduct. In her speech, DAG Yates decried past practices of "limited" disclosure:

Effective immediately, we have revised our policy guidance to require that if a company wants any credit for cooperation, any credit at all, it must identify all individuals involved in the wrongdoing, regardless of their position, status or seniority in the company and provide all relevant facts about their misconduct. It's all or nothing. No more picking and choosing what gets disclosed. No more partial credit for cooperation that doesn't include information about individuals.<sup>19</sup>

DAG Yates noted that while the DOJ has long emphasized the importance of identifying culpable individuals, "until now, companies could

---

18 Yates Memo, at 3-7.

19 Press Release, U.S. Dep't of Justice, Deputy Attorney Gen. Sally Quillian Yates Delivers Remarks at New York University School of Law Announcing New Policy on Individual Liability in Matters of Corporate Wrongdoing (Sept. 10, 2015), *available at* [www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school](http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-new-york-university-school).

cooperate with the government by voluntarily disclosing improper corporate practices, but then stop short of identifying who engaged in the wrongdoing and what exactly they did.”<sup>20</sup> She also emphasized that “we’re not going to let corporations plead ignorance . . . If they want any cooperation credit, they will need to investigate and identify the responsible parties, then provide all non-privileged evidence implicating those individuals.”<sup>21</sup> DOJ attorneys, DAG Yates explained, will be “vigorously testing” the information provided and comparing it to the DOJ’s own investigation to validate its completeness and to ensure that the company does not attempt to minimize the role of any culpable individuals.<sup>22</sup>

Senior DOJ officials have attempted to ease concerns that unlimited investigations will be needed to satisfy the DOJ’s new standard. DAG Yates noted that the DOJ is not asking companies to “boil the ocean.” Rather, the “purpose of this policy is to better identify responsible individuals, not to burden corporations with longer or more expensive internal investigations than necessary . . . We expect thorough investigations tailored to the scope of the wrongdoing.”<sup>23</sup> Just how health care providers should tailor their health care audits or investigations to provide the level of completeness that the DOJ will deem satisfactory is murky, especially given the DOJ’s “all or nothing” standard for cooperation credit.

The reverberations of the Yates Memo have made their way into the health care industry, with attorneys involved in the defense of criminal and civil False Claims Act cases paying close attention to the speeches of DOJ officials in the months following the Yates Memo. On September 22, 2015, Assistant Attorney General (AAG) for the Criminal Division Leslie Caldwell affirmed that “companies seeking cooperation credit must affirmatively work to identify and discover relevant information about culpable individuals through independent, thorough investigations . . . And internal investigations cannot end with a conclu-

---

20 *Id.*

21 *Id.*

22 *Id.*

23 *Id.*

sion of corporate liability, while stopping short of identifying those who committed the criminal conduct.”<sup>24</sup> For those investigations that “will not bear fruit,” Caldwell said a company will be eligible for cooperation credit if it provides the government with relevant facts and otherwise assists in obtaining evidence, even if the company “truly is unable to identify culpable individuals following an appropriately tailored and thorough investigation . . . .”<sup>25</sup> Nonetheless, Caldwell reaffirmed that the DOJ “will carefully scrutinize and test a company’s claims that it could not identify or uncover evidence regarding the culpable individuals, particularly if we are able to do so ourselves.”<sup>26</sup> Caldwell also tried to assuage concerns that the DOJ’s “new guidance does not change existing department policy regarding the attorney-client privilege or work product protection. Prosecutors will not request a corporate waiver of these privileges in connection with a corporation’s cooperation.”<sup>27</sup>

### Reaffirmation of the Yates Memo in May 2016

On May 10, 2016, DAG Yates spoke at the New York City Bar Association White Collar Crime Conference where she again emphasized that the DOJ expects companies to conduct thorough investigations tailored to the scope of the wrongdoing. She recognized how determining the “appropriate scope and how to proceed is always case specific—it’s not possible to lay out hard and fast rules.”<sup>28</sup> DAG Yates reiterated that the DOJ expects that “cooperating companies will continue to turn over the information to the prosecutor as they receive it.”<sup>29</sup> Addressing concerns regarding the attorney-client privilege, she stated that “there is nothing in the Individual Accountability Policy that requires companies to waive

---

24 Press Release, U.S. Dep’t of Justice, Assistant Attorney Gen. Leslie R. Caldwell Delivers Remarks at the Second Annual Global Investigations Review Conference (Sept. 22, 2015), available at [www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-second-annual-global-0](http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-second-annual-global-0).

25 *Id.*

26 *Id.*

27 *Id.*

28 *May 2016 Speech*.

29 *Id.*

attorney-client privilege or in any way rolls back protections already in place. The policy specifically requires only that companies turn over all relevant non-privileged information.”<sup>30</sup> While claiming that defense attorneys’ concerns are exaggerated, the lack of any clear guidance about what constitutes a “complete” internal investigation while trying not to “boil the ocean” leaves health care providers to formulate their own structure.

### The Yates Memo and civil cases

The Yates Memo primarily addressed criminal prosecutions, but its principles have been embraced by agencies involved in civil enforcement cases, especially False Claims Act cases, prevalent in the health care sector. Recent statements have demonstrated that the DOJ intends to pursue civil cases vigorously using the Yates Memo principles. On June 9, 2016, Acting Associate Attorney General Bill Baer extended the “individual accountability” and corporate cooperation standards of the Yates Memo “with equal force and logic to the department’s civil enforcement.”<sup>31</sup> AAG Baer explained how genuine corporate cooperation “involves prompt, no slow-walking, and fulsome, no hiding the ball, responses to government requests for information.”<sup>32</sup> While AAG Baer echoed prior statements about investigations being tailored to the scope of the wrongdoing, the DOJ expects “cooperating companies to make their best effort to determine the facts with the goal of identifying the individuals involved.”<sup>33</sup>

In addition, AAG Baer underscored that timing, meaning early voluntary disclosure, is of the essence and that “[m]aximum credit will be reserved for situations where the company not only fully cooperates but also voluntarily discloses . . . .”<sup>34</sup> He continued that companies should

---

30 *Id.*

31 Press Release, U.S. Dep’t of Justice, Acting Associate Attorney Gen. Bill Baer Delivers Remarks on Individual Accountability at American Bar Association’s 11th National Institute on Civil False Claims Act and Qui Tam Enforcement (June 9, 2016), available at [www.justice.gov/opa/speech/acting-associate-attorney-general-bill-baer-delivers-remarks-individual-accountability](http://www.justice.gov/opa/speech/acting-associate-attorney-general-bill-baer-delivers-remarks-individual-accountability).

32 *Id.*

33 *Id.*

34 *Id.*

understand that “the converse is also true: the conduct of those companies that fail to act promptly, fail to promptly disclose or fail to help us understand who participated in the violation also will be factored into our overall view of the appropriate resolution of the matter.”<sup>35</sup> The message is that if the disclosure is not complete or not voluntary, the prospect of meaningful reduction of penalties or treble damages under the False Claims Act is unlikely.

## The Reverberations of the Yates Memo for Health Care

The DOJ’s heightened emphasis on early voluntary disclosure will increase the need for health care companies to conduct internal investigations when allegations of improper health care practices arise. A key component for the internal investigation is obtaining complete and accurate information from company personnel. Yet, the DOJ’s emphasis on identifying responsible individuals creates potential conflicts of interest with employees or contractors who may be reluctant to cooperate with the company. The Yates Memo may result in employees having to make a Hobbesian choice—either cooperate or face termination or sanctions for a failure to do so.<sup>36</sup> In addition, health care companies will need to collect and assess information when there is a credible allegation of impropriety. The need for internal investigations conducted by experienced counsel should therefore be considered at early stages of allegations. Health care providers should involve external independent counsel to avoid claims that advice and reports by in-house counsel constituted “business advice” and not privileged legal advice.

The Yates Memo, with the DOJ emphasis on cooperation and identification of persons involved, will result in more interaction with prosecutors during the internal investigation. Full cooperation, accord-

---

<sup>35</sup> *Id.*

<sup>36</sup> See *Gilman v. Marsh & McLennan Cos.*, 826 F.3d 69 (2d Cir. 2016) (holding that an employer had cause to terminate two employees for refusing to be interviewed after they were identified as co-conspirators in a criminal bid-rigging scheme).

ing to the DOJ, includes timely updates and production of documents no matter the stage of the internal review. These two factors, which are examples of the company's cooperation obligations under the Yates Memo, necessitate a health care company to strongly consider obtaining separate counsel for employees. While this approach may increase costs, the benefits are significant. Separate counsel will eliminate both the appearance that the company is stifling information and any potential ethical pitfalls. Even if separate counsel represent individual employees, the company's counsel will inevitably have to interview employees as part of the company's internal investigation. Health care companies should therefore expect longer, and likely more costly, internal investigations as a result of the Yates Memo.

While it may increase cooperation with the government, the Yates Memo may impede joint defense agreements between companies, executives, and employees. A joint defense agreement is often used to share privileged information and strategy where the parties have a common interest, such as defending clients in a criminal investigation. Yet, such cooperation between company counsel and individuals' counsel may create the impression of not cooperating fully with the government. This may undermine the willingness of companies to enter into a joint defense agreement. Further, the parties may decide not to share strategy or information out of concern that the company will be asked to divulge information that comes, in part, from employees.

### Increased importance of *Upjohn* warnings to employees

With the Yates Memo's focus on identification of accountable individuals, it is more important than ever to ensure that employees understand the distinction between the company's attorney-client privilege and a personal one. When conducting interviews, counsel should provide *Upjohn* warnings that convey the following key elements:

- The attorney represents the company and is gathering information to provide legal advice to the company.

- The attorney does not represent the employee in his/her personal capacity.
- The attorney is speaking to the employee in his/her capacity as an employee of the company.
- The interview is an attorney-client communication that is privileged, but the holder of the privilege is the company, not the employee.
- The company can disclose what it learns from the employee during interviews without consulting the employee.
- The company can use or disclose to a third party, including the government, the information employee provides, even if it is against the employee's interests.

The central point for *Upjohn* warnings is to ensure that employees understand who the attorney represents. For corporate counsel, the company is the client for purposes of the attorney-client privilege. Employees should understand that interviews and communications are being held solely under the company's privilege, not the employee's privilege. The company, not the individual employee, will make any decision to waive the privilege in order to meet the DOJ's concerns.

Providing *Upjohn* warnings to employees in the post-Yates Memo era will likely result in employees becoming more reluctant to cooperate in investigations, especially without their own counsel. Yet failing to provide *Upjohn* warnings will likely increase the risk that employees will claim information cannot be disclosed because the employee holds the attorney-client privilege. "Watered-down" *Upjohn* warnings, or none at all, could result in a potential legal and ethical mine field.<sup>37</sup> Health care companies should retain separate counsel for employees to allay these concerns. While this practice is not uncommon, health care companies'

---

37 See, e.g., *Butler v. Am. Heritage Life Ins. Co.*, No. 4:13-CV-199 (E.D. Tex. Jan. 29, 2016) (where plaintiff claimed that defendant failed to give *Upjohn* warning in connection with an interview and, therefore, the attorney-client privilege did not attach to any evidence obtained through the interview).



in-house counsel should consider, at the outset of any investigation, finding counsel for employees whose conduct or decisions may be at issue to ensure that no conflicts arise that would interfere with the review.

### Concerns regarding attorney-client privilege and work product protection

Despite the DOJ's denial of any impact on the attorney-client privilege or attorney work product protection, the Yates Memo chips away at the privilege by: (i) not considering the context in which "facts" may become known to counsel and (ii) allowing for a "qualified" or "limited" privilege that equates the attorney-client privilege with the work product doctrine.

The attorney-client privilege protects "communications" with a client in order to foster "full and frank" discussions.<sup>38</sup> The applicability of the attorney-client privilege to internal investigations is well established as "obtaining or providing legal advice was one of the significant purposes" of the communication.<sup>39</sup> In *In re Kellogg Brown and Root*, the D.C. Circuit court found, as did the Supreme Court in *Upjohn*, that the company's privilege claim applied to those facts gathered in an internal investigation.<sup>40</sup> Thus, the privilege protects the giving of professional advice, as well as the factual information obtained from the client that is the basis of the legal advice.<sup>41</sup>

In other words, health care companies have an attorney-client privilege that exists to protect not only the legal advice, "but also the giving of information to the lawyer to enable him to give sound and informed advice."<sup>42</sup> While telling factual information to an attorney does not change otherwise non-privileged information to privileged, the Yates

---

38 *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

39 *In re Kellogg Brown & Root Inc.*, 756 F.3d 754, 760 (D.C. Cir. 2014).

40 *Id.* at 757.

41 *See Upjohn*, at 391.

42 *Id.* at 390.

Memo glosses over the well-settled principle that the attorney-client privilege protects the entire flow of communication, including facts, between attorney and client. Once it is determined that giving or receiving legal advice is the “predominant purpose” of the communication, “other ‘considerations and caveats’ are not severable and the entire communication is privileged.”<sup>43</sup>

The Yates Memo appears to divide the attorney-client privilege into two components: (i) the factual information communicated and (ii) the legal or advice component provided. Under the Yates Memo, the DOJ appears to take the position that the factual component is not privileged and thus, should be disclosed. Yet this approach would nullify the attorney-client privilege, which protects the entire communication, including factual information conveyed to one’s attorney.

While it is too early to tell how the DOJ will apply the new guidance, the Yates Memo signals a more restrictive, and potentially contentious, view of the attorney-client privilege in internal investigations. Companies should be aware of the potential consequences of the government’s steps toward unraveling the attorney-client privilege. As precautionary measures, in-house counsel should document the steps taken to (i) preserve the privilege by separating legal memos and internal investigation documents and (ii) provide legal—not just business—advice about the potential topics for disclosure.

### Impact on administrative actions

One of the greatest risks to a health care entity or practitioner is the threat of being suspended or excluded from participation in federal health care programs. The Office of Inspector General (OIG) is legally required to exclude individuals and entities convicted of the following types of criminal offenses from participation in federal health

---

43 Fox News Network, LLC v. United States Dep’t of the Treasury, 911 F. Supp. 2d 261, 271 (S.D.N.Y. 2012); *see also Upjohn*, at 396.

care programs: (i) Medicare or Medicaid fraud, or any other offense related to the delivery of items or services under Medicare or Medicaid; (ii) patient abuse or neglect; (iii) felony convictions for other health care-related fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct; and (iv) felony convictions for unlawful handling of controlled substances.<sup>44</sup>

The OIG also has discretion to exclude individuals and entities from participation in health care programs on a number of other grounds. On April 18, 2016, the OIG revised its policy statement regarding the non-binding criteria to be used by the OIG in assessing whether to impose exclusion.<sup>45</sup> The OIG's revised policy details two limited circumstances in which the OIG will "usually" give a person a release of exclusion without requiring integrity obligations: (i) when the person self-discloses the fraudulent conduct to the OIG, cooperatively and in good faith, or (ii) when the person agrees to sufficiently robust integrity obligations with a state or the DOJ.<sup>46</sup> These narrow limitations leave the OIG a range of administrative options it can exercise based on the facts and circumstances of each case.

Consistent with the policy changes outlined in the Yates Memo, the OIG has called for increased individual accountability. Recently, the former CEO of Tuomey Healthcare Systems paid \$1 million to resolve his role in Tuomey's illegal compensation arrangements with physicians.<sup>47</sup> Tuomey's former CEO was also excluded for four years from participation in federal health care programs, including providing management or administrative services paid for by federal health care programs.<sup>48</sup> In another case, the board chairman of skilled-nursing facility company North

---

44 42 U.S.C. § 1320a-7.

45 OIG, CRITERIA FOR IMPLEMENTING SECTION 1128(b)(2)(7) EXCLUSION AUTHORITY (Apr. 18, 2016), available at <https://oig.hhs.gov/exclusions/files/1128b7exclusion-criteria.pdf>.

46 *Id.*

47 Press Release, Dep't of Justice, Former Chief Executive of South Carolina Hospital Pays \$1 Million and Agrees to Exclusion to Settle Claims Related to Illegal Payments to Referring Physicians (Sept. 27, 2016), available at <https://www.justice.gov/opa/pr/former-chief-executive-south-carolina-hospital-pays-1-million-and-agrees-exclusion-settle>.

48 *Id.*

American Health Care Inc. (NAHC) paid \$1 million to resolve claims for medically unnecessary rehabilitation services.<sup>49</sup> NAHC's Senior Vice President of Reimbursement Analysis also paid \$500,000 for her role in creating the improper billing scheme.<sup>50</sup>

Because the OIG has discretion to exclude entities from participation in health care programs for a multitude of factors, companies have a strong incentive to assist governmental investigations in hopes of obtaining mitigation credit to offset misdeeds. As under the Yates Memo, to avoid exclusion, health care entities will need to divulge incriminating information about senior executives to avoid allegations that the company reluctantly supported the DOJ's investigation. This will necessarily create an internal conflict within the company as individuals feel pitted against an employer more concerned with cooperation than individual exoneration.

In the health care industry, both employees and employers are well aware that the costs of noncompliance are unquestionably severe. In response to the DOJ's health care fraud enforcement efforts, the Centers for Medicare and Medicaid Services (CMS) have suspended payments to several health care providers based on credible allegations of fraud. In one case, CMS suspended Medicare payments to a Florida cardiologist in March 2015 based on credible allegations that he submitted claims to Medicare for physician services that were not medically reasonable and necessary.<sup>51</sup> The suspension letter issued by CMS noted that, of the 17,258 claims reviewed, 10,057 claims were denied, a 58% denial rate.<sup>52</sup> In addition, the letter provided several examples where the physician billed for over 24 hours of time-based procedure codes on unique dates of service.<sup>53</sup> In another case, CMS suspended Medicare payments to Sacred Heart

---

49 Press Release, Dep't of Justice, North American Health Care Inc. to Pay \$28.5 Million to Settle Claims for Medically Unnecessary Rehabilitation Therapy Services (Sept. 19, 2016), available at [www.justice.gov/opa/pr/north-american-health-care-inc-pay-285-million-settle-claims-medically-unnecessary](http://www.justice.gov/opa/pr/north-american-health-care-inc-pay-285-million-settle-claims-medically-unnecessary).

50 *Id.*

51 CMS, Notice of Suspension of Medicare Payment to Asad Qamar, MD and Institute of Cardiovascular Excellence, PLLC, Mar. 6, 2015 (on file with authors).

52 *Id.* at 3.

53 *Id.* at 5.

Hospital in Chicago in May 2013 as a result of credible allegations that the hospital offered illegal kickbacks in exchange for the referral of hospital patients.<sup>54</sup> Accentuating the severity of CMS's decision to suspend Medicare payments, Sacred Heart Hospital closed shortly after the suspension took effect.<sup>55</sup>

For health care companies subject to the Food Drug & Cosmetic Act (FDCA), exclusions for senior executives may be based on the Responsible Corporate Officer (RCO) doctrine, regardless of whether they actually participated or knew of any violation. The FDCA permits corporate officers to be held criminally liable as “responsible corporate agents” for the failure to prevent or remedy conditions or conduct of subordinates.<sup>56</sup> Even though RCO violations are strict liability misdemeanors, they can be the predicate for exclusions from Medicare or other federal health care programs.<sup>57</sup> In light of the Yates Memo's focus on individual accountability, prosecutions and administrative exclusions of both health care companies and executives based on the RCO doctrine may well increase.

### Increased importance of compliance programs

One of the most significant reverberations from the Yates Memo is the critical importance of compliance programs. DAG Yates declared that “[w]e want to restore and help protect the corporate culture of responsibility. That's only possible with strong compliance programs—and with rigorous internal controls that help companies self-assess and self-correct.”<sup>58</sup>

---

54 Andrew L. Wang & Kristen Schorsch, *Sacred Heart Hospital Closes*, CRAIN'S CHICAGO BUS., July 1, 2013, available at [www.chicagobusiness.com/article/20130701/NEWS03/130709987/sacred-heart-hospital-closes](http://www.chicagobusiness.com/article/20130701/NEWS03/130709987/sacred-heart-hospital-closes).

55 *Id.*

56 *United States v. DeCoster*, No. 15-1890 (8th Cir. July 6, 2016).

57 42 U.S.C. § 1320a-7(b)(1); see *Friedman v. Sebelius*, 686 F.3d 813, 816 (D.C. Cir. 2012).

58 Press Release, U.S. Dep't of Justice, Deputy Attorney General Sally Quillian Yates Delivers Remarks at American Banking Association and American Bar Association Money Laundering Enforcement Conference (Nov. 16, 2015), available at [www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-american-banking-0](http://www.justice.gov/opa/speech/deputy-attorney-general-sally-quillian-yates-delivers-remarks-american-banking-0).

On November 13, 2015, the DOJ hired its first Compliance Officer, Hui Chen, who formerly served as a federal prosecutor and compliance officer at multinational companies in the private sector. Based on her statement, companies must view compliance as an “evolving” process. Ms. Chen emphasized five aspects of an effective compliance program: (i) the design of the program should be tailored to address the problematic areas of the business; (ii) the audit and internal investigations should effectively find and mitigate potential problems; (iii) the communications and culture within the company must encourage employees to raise any concerns; (iv) the company should show both economic and personnel commitment to the compliance program; and (v) the board of directors should be committed and be informed about the compliance programs and potential risks.<sup>59</sup> The DOJ has continued to stress that having a compliance program is not a defense to claims of corporate wrongdoing, but rather a critical factor for a resolution to an investigation.

## Conclusion

The Yates Memo increases the need for health care companies to conduct internal investigations when allegations of improper health care practices arise. While it has long been the DOJ's practice to fully evaluate the evidence in determining both individual and corporate culpability, the Yates Memo embodies the DOJ's fundamental policy shift by requiring corporations to turn over all relevant facts related to individuals responsible for misconduct. Since the turning over of such information is a prerequisite for cooperation credit, the Yates Memo creates a complicated dynamic between any health care company and its employees when noncompliance occurs. Employees will likely be more reluctant to cooperate in investigations. Now, more than ever, health care companies need

---

59 Dep't of Justice, Roundtable Discussion on Compliance with Andrew Weissmann and Hui Chen (Nov. 13, 2015), available at [www.youtube.com/watch?v=pRTGZmmbc5o](http://www.youtube.com/watch?v=pRTGZmmbc5o).

to strongly consider establishing protocols for internal investigations that include obtaining separate counsel for employees.

Although recent DOJ settlements have included settlements with executives, it is too early to assess whether the Yates Memo will increase individual prosecutions or exclusions. While the results are not complete, it is undeniable that the Yates Memo is a firm admonishment that health care companies must develop and adhere to robust compliance programs to meet all areas of business risk. The days of “paper programs” are gone. Both large and small health care companies and their employees must understand their compliance responsibilities in light of the Yates Memo. Failure to do so will leave health care companies and their employees increasingly vulnerable to prosecution.

The change in administrations creates uncertainty regarding how the Yates Memo will be followed. Indeed, DAG Yates addressed this uncertainty in late November 2016 as she tried to forecast its impact. She observed that “individual accountability isn’t a [D]emocratic principle or a [R]epublican principle, but is instead a core value of our criminal justice system that perseveres regardless of which party is in power.”<sup>60</sup> Given Attorney General designate Jeff Sessions’s work as a United States Attorney, it is likely that health care enforcement will remain a top priority. The other lesson of the Yates Memo—the need for a robust compliance program—will certainly continue to have significance.

---

60 Sally Q. Yates, Deputy Attorney Gen., Office of the Deputy Attorney Gen., Remarks at the 33rd Annual International Conference on Foreign Corrupt Practices Act (Nov. 30, 2016), *available at* [www.justice.gov/opa/speech/deputy-attorney-general-sally-q-yates-delivers-remarks-33rd-annual-international](http://www.justice.gov/opa/speech/deputy-attorney-general-sally-q-yates-delivers-remarks-33rd-annual-international).

## 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](http://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](mailto: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](mailto:sbennett@cblawyers.com).

## Rosati and Bennett: Data Breaches

### CONTENTS

Introduction .....	94
HIPAA's Breach Reporting Requirements .....	95
Covered entities: providing notice to individuals, the OCR, and media .....	100
Business associates: when to delegate .....	102
Obtaining law enforcement delay if necessary .....	103
State Breach Reporting Laws .....	103
Coverage of state laws .....	104
Notifications .....	105
Breach Prevention and Preparation .....	106
Have an up-to-date security risk analysis and risk management plan .....	107
Implement a written information security program .....	108
Adopt safeguards to prevent breaches .....	110
Train employees on preventing, recognizing, and reporting breaches.....	111
Adopt and test a breach response plan.....	112
Be proactive with business associates and other vendors .....	115
Establish relationships with organizations that share information on cyber threats.....	119
Ensure adequate cyber insurance coverage.....	120
Responding to a Breach .....	120
Address attorney-client privilege and work product protection .....	121
Instruct personnel to keep information about the breach confidential .....	121
Retain a computer forensic consultant.....	122
Preserve evidence .....	122
Control the damage .....	122

Decide whether to contact law enforcement.....	123
Interview personnel.....	124
Notify insurance carriers.....	124
Decide whether to report the breach .....	124
Prepare for communications with media and other third parties .....	124
Draft notices .....	125
Decide what services to offer affected individuals.....	125
Make logistical arrangements.....	126
Document all steps of the breach response.....	127
Adopt and implement a corrective action plan .....	127
Perform or update the security risk analysis.....	128
Conclusion .....	129

## 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.<sup>1</sup> The average estimated cost of a breach for a health care organization is \$2.2 million.<sup>2</sup> For a business associate, the estimated cost is more than \$1 million.<sup>3</sup> Breaches cost the health care industry an estimated \$6.2 billion every year.<sup>4</sup>

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.<sup>5</sup>

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.<sup>6</sup>

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.idexperts.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm\\_source=Referral&utm\\_medium=press%20release&utm\\_campaign=Ponemon%202016](http://www2.idexperts.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=SELO3094WWEN](http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SELO3094WWEN) [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](http://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.<sup>7</sup>

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,”<sup>8</sup> 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](http://www2.idexpertscorp.com/blog/single/whats-in-a-name-defining-event-vs.-security-incident-vs.-data-breach).

ized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”<sup>9</sup>

Under HIPAA’s Breach Notification Rule, a breach is defined as the unauthorized “acquisition, access, use, or disclosure of protected health information [PHI] in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the [PHI].”<sup>10</sup> Examples of breaches include the loss of an unencrypted thumb drive that contains PHI, a hospital employee snooping through the medical records of a celebrity patient, a doctor’s office disposing of paper records that contain PHI in a publicly accessible dumpster, or hackers accessing PHI in a hospital’s computer system.

Determining whether an incident is a reportable breach under HIPAA requires answering four questions: (i) Was there unauthorized acquisition of, access to, or use or disclosure of PHI? (ii) Was the PHI unsecured? (iii) Does an exception to the definition of breach apply? (iv) Can the covered entity or business associate demonstrate a “low probability that the PHI has been compromised?”<sup>11</sup>

First, it is important to note that a violation of the Security Rule does not, by itself, create a reporting obligation unless the violation causes an unauthorized use or disclosure of PHI. As just one example, the Security Rule requires covered entities and business associates to perform a periodic evaluation to determine whether their policies and procedures meet the requirements of the Rule.<sup>12</sup> A failure to conduct that evaluation would not, by itself, constitute a reportable breach.

Second, HIPAA requires notifications for breaches of “unsecured” PHI.<sup>13</sup> PHI is secure if it has been “rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary [of Health and Human

---

9 45 C.F.R. § 164.304.

10 45 C.F.R. § 164.402.

11 *Id.*

12 *Id.* § 164.308(a)(8).

13 *Id.* §§ 164.404(a)(1), .406(a), .408(a), .410(a)(1).

Services (HHS)]. . . .”<sup>14</sup> PHI is considered secure for purposes of the Breach Notification Rule if it has been encrypted according to standards issued by the National Institute of Standards and Technology, or if the media on which the PHI was stored has been destroyed as specified.<sup>15</sup> If the PHI was secured accordingly, no reporting is required. If, however, PHI was unsecured, the entity must proceed to the third question.

Although encryption of devices and data helps to avoid a reportable breach, the OCR has noted the limits of full or whole disk encryption. Full disk encryption “encrypts the entire disk including swap files, system files, and hibernation files. If an encrypted disk is lost, stolen, or placed into another computer, the encrypted state of the drive remains unchanged, and only an authorized user can access its contents.”<sup>16</sup> In July 2016 guidance regarding ransomware, the OCR cautioned that full disk encryption makes the data on a hard drive secure only when the system is powered down.<sup>17</sup> “Once the computer system is powered on and the operating system is loaded, . . . many full disk encryption solutions will transparently decrypt and encrypt files accessed by the user.”<sup>18</sup>

This means if a laptop with full disk encryption is powered off, and is then lost or stolen, the data on the hard drive would be considered secure PHI, so the incident would not be a reportable breach under HIPAA.<sup>19</sup> In contrast, if the laptop “is powered on and in use by an authenticated user,” and the laptop is lost, stolen, or attacked by ransomware, any PHI on the laptop would not be secure, so reporting might be

---

14 *Id.* § 164.402 (defining *unsecured* PHI).

15 OCR, *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, HHS.gov, [www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html](http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html) (last visited Nov. 20, 2016).

16 SYMANTEC, WHITE PAPER: HOW WHOLE DISK ENCRYPTION WORKS 1 (2010), available at [www.symantec.com/content/en/us/enterprise/white\\_papers/b-gpg\\_how\\_wholedisk\\_encryption\\_works\\_WP\\_21158817-en-us.pdf](http://www.symantec.com/content/en/us/enterprise/white_papers/b-gpg_how_wholedisk_encryption_works_WP_21158817-en-us.pdf) [hereinafter WHITE PAPER: HOW WHOLE DISK ENCRYPTION WORKS].

17 OCR, FACT SHEET: RANSOMWARE AND HIPAA 8, available at [www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf](http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf) [hereinafter FACT SHEET: RANSOMWARE AND HIPAA].

18 *Id.*

19 *Id.*

required.<sup>20</sup> In that situation, the data on the laptop would be considered secure only if the individual files were encrypted.<sup>21</sup>

Third, HIPAA's Breach Notification Rule excludes three situations from the definition of breach:

1. The unintentional acquisition, access, or use of PHI by a work-force member.
2. An inadvertent disclosure of PHI by an authorized person to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement.
3. Disclosures of PHI where the entity has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

If one of the three exceptions applies, the covered entity or business associate should document that determination, and notification is not required.<sup>22</sup>

Finally, if no exception applies, unauthorized acquisition of, access to, or use or disclosure of unsecured PHI is presumed to be a breach unless the covered entity or business associate "demonstrates that there is a low probability that the protected health information has been compromised . . . ."<sup>23</sup> The covered entity or business associate must assess all relevant factors, including at a minimum the following four factors:<sup>24</sup>

1. **The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification:** Could the information, such as social security number or birth date, be

---

20 *Id.*

21 WHITE PAPER: HOW WHOLE DISK ENCRYPTION WORKS, at 1 (explaining the difference between whole disk and file encryption).

22 45 C.F.R. § 164.402(1).

23 *Id.* § 164.402(2).

24 *Id.* § 164.402(2)(i)–(iv).



used in a way that harms the individual (e.g., to commit identify theft)?

2. **The unauthorized person who used the PHI or to whom the disclosure was made:** For example, if the PHI was impermissibly disclosed to another HIPAA-obligated entity, there might be a lower probability that the PHI has been compromised.<sup>25</sup>
3. **Whether the PHI was actually acquired or viewed:** For example, if a forensic analysis shows that the PHI on a lost and recovered computer was never accessed or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual, even though the opportunity existed.<sup>26</sup> (Note that the OCR has stated that an entity may not unduly delay reporting to conduct forensic analysis on a recovered laptop.<sup>27</sup>)
4. **The extent to which the risk to the PHI has been mitigated:** For example, the covered entity or business associate could obtain the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means), or that it will be returned or destroyed.<sup>28</sup>

In July 2016, the OCR issued guidance stating that this same four-factor risk assessment is required for ransomware attacks, which are an increasing threat for health care organizations.<sup>29</sup> The OCR stated:

---

25 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; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5643 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

26 *Id.*

27 *Id.* at 5646.

28 *Id.* at 5643.

29 Jocelyn Samuels, *Your Money or Your PHI: New Guidance on Ransomware*, HHS.GOV, July 11, 2016, [www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html](http://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html); FACT SHEET: RANSOMWARE AND HIPAA; see also Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED, Mar. 30, 2016, [www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/](http://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/).

“When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a ‘disclosure’ not permitted under the HIPAA Privacy Rule.”<sup>30</sup> The OCR will presume that a ransomware incident is a reportable breach “[u]nless the covered entity or business associate can demonstrate that there is a ‘ . . . low probability that the PHI has been compromised,’ based on the factors set forth in the Breach Notification Rule . . . .”<sup>31</sup>

Covered entities and business associates bear the burden of proof when it comes to demonstrating that an incident results in a low probability of compromise.<sup>32</sup> If the entity concludes there is a low probability, it should document its reasons. A covered entity or business associate may also opt to provide notice without conducting a risk assessment.<sup>33</sup>

### Covered entities: providing notice to individuals, the OCR, and media

A HIPAA-covered entity must provide notice to “each individual whose unsecured protected health information has been, or is reasonably believed . . . to have been, accessed, acquired, used, or disclosed as a result of such breach.”<sup>34</sup> The notice must be in writing and sent by first-class mail, or by e-mail if the affected individual has agreed to electronic notice.<sup>35</sup>

If the covered entity has insufficient contact information for fewer than 10 individuals, the entity may provide substitute notice by alternative written notice, telephone, or other means.<sup>36</sup> If the covered entity has insufficient contact information for 10 or more individuals, the entity must

---

30 FACT SHEET: RANSOMWARE AND HIPAA. at 5–6.

31 *Id.* at 6.

32 45 C.F.R. § 164.414(b).

33 78 Fed. Reg. at 5643.

34 45 C.F.R. § 164.404(a)(1).

35 *Id.* § 164.404(d).

36 *Id.* § 164.404(d)(2)(i)-(ii).

provide substitute notice by either posting the notification on the home page of its website (for at least 90 days) or by providing the notice in major print or broadcast media where the affected individuals likely reside.<sup>37</sup> The covered entity must also include a toll-free phone number that individuals can access for at least 90 days to learn more about the incident.<sup>38</sup>

Based on the authors' experience, in nearly every significant breach, the entity will lack accurate contact information for 10 or more people. Entities should therefore assume they need to provide substitute notice, unless proven otherwise.

Individual notification must be provided to affected individuals without unreasonable delay, and no later than 60 days following discovery of the breach.<sup>39</sup> A breach is "discovered" as of the first day on which the incident is known or should reasonably have been known to the covered entity.<sup>40</sup> (Some states' laws might require a shorter reporting period, as discussed [later](#).)

A covered entity also must notify the OCR of every breach of unsecured PHI via an online form.<sup>41</sup> If a breach affects 500 or more individuals, covered entities must notify the OCR at the same time that they notify affected individuals.<sup>42</sup> Breaches of 500 or more are posted on the OCR's website,<sup>43</sup> known in the industry as the "Wall of Shame." If a breach affects fewer than 500 individuals, the covered entity may notify the OCR of all such breaches annually.<sup>44</sup>

Finally, if a covered entity experiences a breach that affects more than 500 residents of a particular state or jurisdiction, the entity must provide

---

37 *Id.* § 164.404(d)(2)(ii).

38 *Id.* § 164.404(d)(2)(ii).

39 *Id.* § 164.404(a)(1) & (b).

40 *Id.* § 164.404(a)(2).

41 *Id.* § 164.408; OCR, *Breach Reporting*, HHS.gov, [www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/](http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/) (last visited Nov. 20, 2016).

42 45 C.F.R. § 164.408(a).

43 OCR, *Breaches Affecting 500 or More Individuals*, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (last visited Nov. 20, 2016).

44 45 C.F.R. § 164.408(b).

notice to “prominent media outlets” serving that state or jurisdiction.<sup>45</sup> The OCR has explained, however, that breaches involving residents of multiple states might not require media notice. For example, if a covered entity discovers a breach of 700 individuals, 300 from Illinois, 300 from Wisconsin, and 100 from Ohio, the breach would not affect more than 500 residents of any one state or jurisdiction, and therefore media notice would not be required.<sup>46</sup> Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, a prominent media outlet may be a major general interest newspaper that circulates daily throughout the city, rather than the entire state.<sup>47</sup>

Entities could consider providing media notice in a manner that also meets the requirements of substitute notice, which are slightly different. Like individual notice, notice to the media must be provided without unreasonable delay, and in no case later than 60 days following the discovery of a breach. The notice must include the same content required for notification to individuals.<sup>48</sup> Notice to the media does not have to be concurrent with notice to individuals, which provides time to notify individuals before making the breach public.

### Business associates: when to delegate

The covered entity is ultimately responsible for ensuring that all required notifications are provided, but it may delegate the task of providing notice to a business associate responsible for the breach.<sup>49</sup> In allocating notice responsibility, organizations should consider which entity has the relationship with the affected individuals.<sup>50</sup> If the covered entity has the primary relationship (the most common situation), the covered entity likely will want to notify affected individuals. When a business associate’s breach affects numerous covered entities, it might

---

45 *Id.* § 164.406(a).

46 78 Fed. Reg. at 5653.

47 *Id.*

48 45 C.F.R. § 164.406(c).

49 78 Fed. Reg. at 5650.

50 *Id.* at 5651.

be preferable for the business associate to provide the notice, so that affected individuals receive just one notification. This might occur, for example, in the context of a health information exchange where the breach compromises a repository that contains the PHI of several covered entities.

### Obtaining law enforcement delay if necessary

Both covered entities and business associates may delay required notifications at the request of law enforcement, if giving notice would interfere with a criminal investigation or harm national security.<sup>51</sup> If the request is in writing and specifies a time period, the covered entity or business associate must delay notice for that period.<sup>52</sup> If the request is verbal, the covered entity or business associate may delay notice for no more than 30 days and must document the request and the identity of the requesting official.<sup>53</sup> Organizations should ask law enforcement to provide a written request and retain all documentation so they can demonstrate to the OCR that notifications were timely.

Organizations should also be prepared to explain to law enforcement why a delay would benefit the agency's investigation, and not just the organization. Until law enforcement requests a delay, organizations should proceed under the assumption that notifications must be made by the default deadlines under HIPAA and state law.

## State Breach Reporting Laws

Currently, 47 states—as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands—have laws that require reporting of certain breaches involving personally identifiable information. (As of this writing, Alabama, New Mexico, and South Carolina are the only

---

<sup>51</sup> 45 C.F.R. § 164.412.

<sup>52</sup> *Id.* § 164.412(a).

<sup>53</sup> *Id.* § 164.412(b).

states with no breach reporting laws.)<sup>54</sup> Given the variation in states' breach laws, it is critical to assess an organization's obligations under the laws of each relevant state. State law might, for example, require reporting of breaches of personal information beyond PHI; impose shorter reporting timeframes; require notification of additional entities; and mandate different content in the written notice. There are print and online resources that summarize the various state reporting laws, but those laws can change quickly, so when dealing with a breach, it is important to review primary sources of authority.

### Coverage of state laws

Some state laws have limited coverage, applying only to a person or entity that does business in that state.<sup>55</sup> Others apply to any person or entity that holds personal information of that state's residents.<sup>56</sup> An attempt by one state to regulate conduct that occurs outside its borders raises potential legal problems, such as under the due process and dormant commerce clauses of the U.S. Constitution.<sup>57</sup> To the authors' knowledge, no court has determined the constitutionality of state breach statutes that attempt to regulate out-of-state businesses. In addition, some state laws exempt organizations subject to federal regulation, such as covered entities or business associates under HIPAA, or financial institutions subject to the Gramm-Leach-Bliley Act.<sup>58</sup> Most states require notification to only their affected residents, but some states require notice to *all* affected people.<sup>59</sup>

---

54 For the citations to all state breach reporting laws that were in effect as of January 1, 2016, see *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES, Jan. 4, 2016, [www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx](http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx); see also JONATHAN M. JOSEPH, *AHLA DATA BREACH NOTIFICATION LAWS: A FIFTY STATE SURVEY*, SECOND EDITION (American Health Lawyers Association 2d ed.).

55 See, e.g., CONN. GEN. STAT. § 36a-701b(b)(1).

56 See, e.g., MASS. GEN. LAWS ch. 93H, § 3(b).

57 See, e.g., Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 FED. COMM. L. J. 409, 411 (2014-15), available at [www.fclj.org/wp-content/uploads/2016/01/67.3.2-Glosson.pdf](http://www.fclj.org/wp-content/uploads/2016/01/67.3.2-Glosson.pdf).

58 See, e.g., ARK. CODE § 4-110-106; WIS. STAT. § 134.98(3m).

59 See, e.g., HAW. REV. STAT. § 487N-2(a); N.H. REV. STAT. §§ 359-C:20(l)(a); N.C. GEN. STAT. § 75-65(a); TEX. BUS. & COM. CODE § 521.053(b).

## Notifications

Most states put the burden of notifying affected individuals on the person or entity that owns or leases the data. A person or entity that is simply maintaining the data is generally required only to notify the owner.<sup>60</sup> Some states require reporting to state regulators (generally, the state's attorney general), or the three credit reporting agencies if the breach exceeds a certain size.<sup>61</sup>

States generally require notifications of breaches involving a person's name, in combination with any of the following:

1. social security number;
2. driver's license or state ID card number; or
3. credit card number, debit card number, or financial account number, in combination with any password, security code or access code that would allow access to the account.<sup>62</sup>

Some states require notification for breaches of other types of information, including biometrics, taxpayer ID numbers, birth certificates, and medical information.

Nearly every state has a safe harbor (i.e., reporting is not required) if the personal information was encrypted or redacted.<sup>63</sup> The notable exception is Tennessee, which in 2016 modified its breach statute to eliminate the safe harbor for encrypted information.<sup>64</sup> Some states have harm thresholds for reporting, which generally provide that reporting is not required if the breached entity determines there is no reasonable likelihood of harm to consumers or misuse of personal information.<sup>65</sup>

---

60 See, e.g., UTAH CODE § 13-44-202(3)(b).

61 See, e.g., FLA. STAT. § 501.171(3) & (5).

62 See, e.g., DEL. CODE tit. 6, § 12B-101(4).

63 See, e.g., Cal. Civ. Code § 1798.81.5 (d)(1)(A).

64 TENN. CODE § 47-18-2107.

65 See, e.g., MICH. COMP. LAWS § 445.72(1); KAN. STAT. § 50-7a01(a).

Many states require reporting “in the most expedient time possible and without unreasonable delay . . . .”<sup>66</sup> Some states have imposed specific time limits.<sup>67</sup> The current shortest time period is under California law, which requires notice of health care breaches within 15 business days.<sup>68</sup> States generally allow a breached entity to delay notifications at the request of law enforcement.<sup>69</sup>

State laws vary significantly when it comes to the content of notices. Some have no requirements, leaving it up to the breached entity,<sup>70</sup> while others mandate specific content.<sup>71</sup> Still others *prohibit* certain information in the notices to individuals. Massachusetts forbids including information about the nature of the breach, and both Massachusetts and Illinois bar entities from disclosing the number of people affected.<sup>72</sup> For breaches of unsecured PHI subject to HIPAA, the restrictions under Massachusetts and Illinois law are likely preempted to the extent they conflict with HIPAA’s requirements.<sup>73</sup>

Some states allow email notice under certain circumstances,<sup>74</sup> and most states allow substitute notice (i.e., some combination of email, website posting, and media notice) if the breach exceeds a certain size in terms of cost or number of individuals affected.<sup>75</sup>

## Breach Prevention and Preparation

Due to the significant likelihood that any given organization will experience a data breach, preparation is critical. One study found that improvements in data governance (such as incident response plans, appointing a chief information security officer, and employee training

---

66 See, e.g., GA. CODE § 10-1-912(a).

67 See, e.g., FLA. STAT. § 501.171(4)(d).

68 CAL. HEALTH & SAFETY CODE § 1280.15(b).

69 See, e.g., CONN. GEN. STAT. § 36a-701b(d).

70 See, e.g., IDAHO CODE § 28-51-105.

71 See, e.g., MD. CODE COM. LAW § 14-3504(g).

72 MASS. GEN. LAWS ch. 93H, §3(a); 815 ILL. COMP. STAT. 530/10(a).

73 See 45 C.F.R. § 160.203 (HIPAA’s preemption provision).

74 See, e.g., LA. STAT. § 51:3074(E).

75 See, e.g., MINN. STAT. § 325E.61(g).



and awareness programs) and investments in technological solutions (e.g., data loss prevention software, encryption, and endpoint security) significantly reduce the costs of a data breach.<sup>76</sup>

### Have an up-to-date security risk analysis and risk management plan

Conducting an in-depth inventory of the organization's data (type of data, where it resides, who has access) and analyzing the risks to that data constitute the basic building blocks of a good security program. The HIPAA Security Rule requires covered entities and business associates to have a current security risk analysis that is "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization] . . . ."<sup>77</sup>

Guidance to help organizations perform a risk assessment is available from the OCR,<sup>78</sup> the Centers for Medicare and Medicaid Services (CMS),<sup>79</sup> the Office of the National Coordinator for Health Information Technology (in partnership with the OCR),<sup>80</sup> and the National Institute of Standards and Technology.<sup>81</sup>

After the risk analysis is complete, the next step is to create and put into practice a risk management plan. The HIPAA Security Rule states that entities must "[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level . . . ."<sup>82</sup>

---

76 2016 COST OF DATA BREACH STUDY, at 2.

77 45 C.F.R. § 164.308(a)(1)(ii)(A).

78 OCR, *Final Guidance on Risk Analysis*, HHS.GOV, [www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html](http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html) (last visited Nov. 20, 2016) [hereinafter *Final Guidance on Risk Analysis*].

79 CMS, *6 Basics of Risk Analysis and Risk Management*, 2 HIPAA SECURITY SERIES (2007), available at [www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf](http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf) [hereinafter HIPAA SECURITY SERIES].

80 *Security Risk Assessment Tool*, HEALTHIT.GOV, [www.healthit.gov/providers-professionals/security-risk-assessment-tool](http://www.healthit.gov/providers-professionals/security-risk-assessment-tool) (last updated Oct. 13, 2016).

81 Nat'l Inst. of Standards & Tech., *Cybersecurity Framework*, [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework) (last visited Nov. 20, 2016).

82 45 C.F.R. § 164.308(a)(1)(ii)(B).

CMS published guidance on implementing a risk management plan.<sup>83</sup> A written risk management plan should address the gaps identified in the risk analysis, include specific tasks to address those gaps, create a timeline, and identify the person responsible for each task.

The security risk analysis and risk management plan should be reviewed and updated periodically and every time there is a material change to the organization's security environment.<sup>84</sup> According to the OCR, "if the covered entity has experienced a security incident, has had change in ownership, turnover in key staff or management, is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected."<sup>85</sup> Health care organizations should integrate the process for updating the security risk analysis and risk management plan into a written information security program.

### Implement a written information security program

It is standard business practice to have a written information security program (WISP) that "documents the measures that a business, or organization, takes to protect the security, confidentiality, integrity, and availability of the personal information and other sensitive information it collects, creates, uses, and maintains . . . ."<sup>86</sup> The organization's risk management plan can be included in the WISP. Sample WISPs are available for free online, providing a useful starting point for health care organizations looking to develop their own.<sup>87</sup>

---

83 *Final Guidance on Risk Analysis*; HIPAA SECURITY SERIES.

84 45 C.F.R. §§ 164.306(e), .316(b)(2)(iii).

85 OCR, *Guidance on Risk Analysis*, HHS.gov, [www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html](http://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html) (last visited Nov. 20, 2016).

86 MELISSA KRASNOW, WRITTEN INFORMATION SECURITY PROGRAM (WISP), PRACTICAL LAW, at 1, *available at* [https://iapp.org/media/pdf/resource\\_center/Krasnow\\_model\\_WISP.pdf](https://iapp.org/media/pdf/resource_center/Krasnow_model_WISP.pdf) [hereinafter WRITTEN INFORMATION SECURITY PROGRAM].

87 *See* WRITTEN INFORMATION SECURITY PROGRAM; COMMONWEALTH OF MASS., OFFICE OF CONSUMER AFFAIRS & BUS. REGULATION, A SMALL BUSINESS GUIDE: FORMULATING A COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM, *available at* [www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf](http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf) [hereinafter A SMALL BUSINESS GUIDE].

Although the HIPAA Security Rule does not use the term WISP, that is effectively what the Rule requires. Under the Security Rule, both covered entities and business associates must “[i]mplement reasonable and appropriate policies and procedures to comply with [the requirements of the Security Rule].”<sup>88</sup> Those requirements include taking steps to “[e]nsure the confidentiality, integrity, and availability of all electronic PHI [ePHI],” and to protect against “reasonably anticipated” threats, hazards, or unauthorized uses or disclosures of ePHI.<sup>89</sup>

The content of a WISP depends on the nature and size of the business. WISPs for health care organizations generally should include:<sup>90</sup>

- Administrative, technical, and physical safeguards to keep information secure
- A process to identify, on a periodic basis, internal and external threats to information
- A process to manage identified threats
- The identity of the specific employee responsible for maintaining and implementing security policies
- Description of the types of sensitive information maintained by the organization
- Where and how sensitive information is stored
- How sensitive information may be transferred out of the organization
- Procedures for:
  - Username and password assignment

*list continues*

---

88 45 C.F.R. § 164.316(a).

89 *Id.* § 164.306(a)(1).

90 See WRITTEN INFORMATION SECURITY PROGRAM; A SMALL BUSINESS GUIDE; JENA VALDETERO & DAVID ZETOONY, WASH. LEGAL FOUND., DATA SECURITY BREACHES: INCIDENT PREPAREDNESS AND RESPONSE 16–17 (2014), available at [www.bryancave.com/images/content/2/2/v2/2285/DataBreach-HandbookValdeteroandZetoon.pdf](http://www.bryancave.com/images/content/2/2/v2/2285/DataBreach-HandbookValdeteroandZetoon.pdf) [hereinafter DATA SECURITY BREACHES: INCIDENT PREPAREDNESS AND RESPONSE].

- Password strength and periodic changes
- Encryption, including which devices and data must be encrypted, and encryption standards for data in transit and data at rest
- Granting and de-activating user credentials
- Employee training on security
- Destroying data
- Retaining vendors that will have access to sensitive data
- Disciplinary measures for security violations
- A process for regularly reviewing and updating the program, including the identity of the person responsible

### Adopt safeguards to prevent breaches

A few safeguards deserve discussion because they can prevent many data breaches.<sup>91</sup> First, organizations should encrypt devices (especially mobile devices) and data where practicable to take advantage of the reporting “safe harbor” under HIPAA and many state reporting laws. A 2016 study of data breaches showed that encryption reduced the cost of a data breach by \$13 per compromised record.<sup>92</sup>

Organizations should consider investing in robust electronic logging features. Logging might help an organization prove that a security incident did not lead to actual exfiltration (removal) of data, allowing it to avoid the substantial cost associated with breach reporting. Special attention should be paid to logging during any transition to new software, which can create gaps in log coverage that compromise subsequent forensic investigations.

---

91 See generally FTC, *START WITH SECURITY: A GUIDE FOR BUSINESS: LESSONS LEARNED FROM FTC CASES* (2015), available at [www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf](http://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf).

92 2016 COST OF DATA BREACH STUDY, at 14.

Health care organizations should take measures to protect passwords, prohibiting employees from using the same password for work and personal accounts, mandating strong passwords through a combination of policies and technology, prohibiting employees from storing passwords near computers or devices, and prohibiting personnel from sharing passwords with others.

Finally, organizations should limit information collected and retain only data that is needed. Regularly reviewing and implementing data-destruction policies will help secure devices and systems no longer in use. Organizations should limit employees' access to only the electronic files, paper documents, and physical locations necessary for their jobs. There should be a process to revisit employees' access when they change roles, and to remove access when they leave the organization.

### Train employees on preventing, recognizing, and reporting breaches

One 2016 study of health care organizations found: "While external threats dominate, internal problems such as mistakes—unintentional employee actions, third-party snafus, and stolen computing devices—are equally a problem and account for a significant percentage of data breaches. In fact, 36% of healthcare organizations and 55% of BAs named unintentional employee action as a breach cause."<sup>93</sup> A 2016 study of data breaches showed that employee training on information security reduced the cost of a data breach by \$9 per compromised record.<sup>94</sup>

---

93 PONEMON INST., SIXTH ANNUAL BENCHMARK STUDY ON PRIVACY & SECURITY OF HEALTHCARE DATA 1, 2 (2016), available at [www2.idexperts.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm\\_source=Referral&utm\\_medium=press%20release&utm\\_campaign=Ponemon%202016](http://www2.idexperts.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]; see also VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT 20 ("63% of confirmed data breaches involved weak, default or stolen passwords"), available at [www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2016\\_Report\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf); 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-health-care-total-over-112-million-records-in-2015/#1fd6afb47fd5](http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-health-care-total-over-112-million-records-in-2015/#1fd6afb47fd5) ("[P]eople are still often the weakest link in the security equation. The truth is that it doesn't matter how strong your security is, people still need to be trained properly on how to protect data.").

94 2016 COST OF DATA BREACH STUDY, at 14.

Organizations need to train personnel on privacy and security<sup>95</sup> when they are first hired and at least annually after. Training should include information about the organization's privacy and security policies, including the WISP, incident response plan, and breach response plan (if it is not part of the incident response plan), as well as practical information about who to contact if an employee suspects a breach or has questions. Personnel should be reminded that violations of privacy and security policies can lead to employee discipline, as well as other real and personal consequences, such as when the direct-deposit paychecks of a university professor were rerouted by hackers.<sup>96</sup>

Employee training should include information about *good security hygiene*. Entities should also consider providing ongoing regular privacy and security education and reminders outside of formal training, such as emailing monthly privacy and security tips to all personnel and sharing free, online security resources.<sup>97</sup>

### Adopt and test a breach response plan

Health care organizations should establish a breach response team of internal personnel who can bring in outside experts as necessary. A 2016 study of data breaches showed that having a response team reduced the cost of a data breach by \$16 per compromised record.<sup>98</sup> An established breach response team can make the breach response faster, more effective, and less stressful for everyone involved.

A response plan can help employees understand their own roles, the roles of other team members, and what they should do (or not do) when

---

95 See 45 C.F.R. § 164.308(a)(5)(i).

96 Darlene Storm, Opinion, *Hacker Steals Teacher's Direct Deposit Paycheck: University Says Too Bad So Sad*, COMPUTERWORLD (Feb. 3, 2014, 6:00 AM), [www.computerworld.com/article/2475732/cybercrime-hacking/hacker-steals-teacher-s-direct-deposit-paycheck-university-says-too-bad-so-sad.html](http://www.computerworld.com/article/2475732/cybercrime-hacking/hacker-steals-teacher-s-direct-deposit-paycheck-university-says-too-bad-so-sad.html).

97 See, e.g., MIT Info. Sys. & Tech., *Top Ten Safe Computing Tips*, <https://ist.mit.edu/security/tips> (last visited Nov. 24, 2016); U.S. Small Bus. Admin., *Top Ten Cybersecurity Tips*, [www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips](http://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips) (last visited Nov. 24, 2016).

98 2016 COST OF DATA BREACH STUDY, at 14.

responding to a security incident or potential breach. A plan's format and content will depend on the size and nature of the entity, but every plan should be specific and actionable, addressing the following points for investigating a potential breach:<sup>99</sup>

- Define triggering events, such as “security incident” and “breach.”
- Identify all members of the incident response team, with 24/7 contact information and alternate team members in case designated members are not available. Most health care organizations choose to include representatives of IT, legal, risk management, operations, marketing/communications, finance, audit, and human resources (if the incident involves employee misconduct or affects employees' personal information).
- Include a plan for covering the normal job responsibilities of the team members who are handling the incident.
- Clarify who is responsible for conducting the investigation and response, including:
  - The role of each team member.
  - Who is in charge of each aspect of the incident response.
  - To whom and when information about the incident should be reported.

*list continues*

---

99 See, e.g., CYBERSECURITY UNIT, COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS 2–3 (2015), available at [www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal\\_division\\_guidance\\_on\\_best\\_practices\\_for\\_victim\\_response\\_and\\_reporting\\_cyber\\_incidents2.pdf](http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf) [hereinafter BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS]; DATA SECURITY BREACHES: INCIDENT PREPAREDNESS AND RESPONSE, at 18–20; INCIDENT RESPONSE PLAN EXAMPLE, available at [www.cio.ca.gov/ois/government/library/documents/incident\\_response\\_plan\\_example.doc](http://www.cio.ca.gov/ois/government/library/documents/incident_response_plan_example.doc).

- Criteria and timelines for escalating the incident to management.
- Who has the authority and responsibility to seek additional personnel or resources.
- The role of in-house and/or outside counsel, and the process for maximizing the potential to protect the investigation under the attorney-client privilege and work product doctrine.
- Contain instructions on how to preserve evidence, including preserving electronic evidence in a forensically sound manner.
- Prohibit actions that might compromise the breach response. For example, personnel should not make changes to devices or computer systems without the guidance of a forensic consultant or qualified IT expert. Personnel should not attempt to “hack back” into a third-party system that appears to be the source of a cyber-attack.
- Clarify recordkeeping and documentation requirements, including who is responsible, what must be documented, and how long and where documentation must be retained.
- Include a process for post-incident reports to management and self-assessment.

Response plans should also include the following points for those events that the organization determines constitute a breach:

- The organization’s policy on breach reporting. This includes addressing who has the authority to decide whether to notify affected individuals, data owners, regulators, the media, law enforcement, and other third parties (such as organizations that share information about cyber threats).
- An alternative communication process. For example, if investigators do not want the hackers to know the organization is aware of the hacking incident (so that the hackers don’t create



additional back doors to the system), organizations might use personal emails and cell phone numbers during the initial parts of the breach investigation.

- Contact information for third parties who will be involved in breach response, such as outside counsel; forensic consultants; call center staffing; law enforcement; and vendors who will perform data clean-up, produce and mail letters, and provide credit monitoring and identity protection services.<sup>100</sup>
- A summary of the entity's contractual reporting obligations, including what types of incidents must be reported, the timeline for reporting, and the name and contact information of the person who must receive the report. (This is especially important to business associates.)

At least once a year, the team members should participate in a table-top drill where they practice responding to a simulated incident. That will allow team members to get comfortable with their roles and the other team members. It can also help identify areas where the response plan can be improved.

### Be proactive with business associates and other vendors

In one 2016 study, 41% of health care organizations reported that they had a breach caused by a third party.<sup>101</sup> An organization needs to look beyond the security of its own information systems and employees and examine vendors who have access to or host the organization's data. That includes billing companies, accountants, attorneys, document storage and shredding companies, and cloud storage providers. Under both HIPAA and state breach laws, organizations are responsible for reporting breaches by third parties in possession of the organizations'

---

100 Organizations should consider identifying or even contracting with vendors in advance of a breach. It might allow the organization to negotiate better rates.

101 SIXTH ANNUAL BENCHMARK STUDY ON PRIVACY & SECURITY OF HEALTHCARE DATA, at 2.

PHI or personal information. Breaches by third parties can also lead to lawsuits against the organization, government investigations, and fines.

Organizations can reduce the risk by vetting vendors' privacy and security practices, and putting protective measures in vendor contracts. HIPAA requires covered entities and business associates to enter into written business associate agreements (BAAs), and requires certain content in those agreements.<sup>102</sup> Although HIPAA applies to a covered entity's relationship with only vendors that use or disclose the entity's PHI, the information handling and reporting requirements of a BAA are a good starting point for written agreements with all vendors that will receive sensitive information.

HIPAA does not, however, address all important aspects of the covered entity-BAA relationship, such as financial responsibility for breaches. Organizations should therefore go beyond HIPAA's requirements of a BAA and address the following issues in vendor contracts:<sup>103</sup>

- Specify how to communicate security incidents and breaches:
  - What types of incidents the vendor must report to the organization. Entities might consider requiring reporting of all suspected security incidents or breaches, so that the vendor is not responsible for determining whether there is a reportable event.
  - The timeline for vendor reporting. Making the timeline short allows the covered entity more time to conduct an adequate

---

102 The website of the OCR includes a sample business associate agreement that includes all of the provisions required by HIPAA. U.S. Dep't of Health & Human Servs., *Business Associate Contracts: Sample Business Associate Agreement Provisions*, HHS.gov (Published Jan. 25, 2013), [www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html](http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html).

103 See generally AHA, ATTACHMENT TO AHA LEGAL ADVISORY: BUSINESS ASSOCIATE AGREEMENT: A CHECKLIST OF REQUIRED AND OPTIONAL PROVISIONS, *available at* [www.aha.org/content/00-10/ChecklistOfReqOptElements092302.pdf](http://www.aha.org/content/00-10/ChecklistOfReqOptElements092302.pdf); Ober Kaler, PREPARING FOR THE HITECH SEPTEMBER DEADLINE: TIPS FOR NEGOTIATING EFFECTIVE BUSINESS ASSOCIATE AGREEMENTS UNDER HIPAA (July 29, 2014), *available at* [www.bakerdonelson.com/2673-webinar-preparing-hitech-september-deadline-tips-negotiating-effective](http://www.bakerdonelson.com/2673-webinar-preparing-hitech-september-deadline-tips-negotiating-effective).

investigation or oversee the business associate's investigation. Quick reporting also may help mitigate any potential damages by allowing affected people to promptly obtain identity theft protection services.

- The name and contact information of the representative who should receive the vendor's report, and the information the vendor must include in the report. HIPAA requires certain information for breaches of unsecured PHI,<sup>104</sup> but the entity might want to require a report of the types of PHI or other sensitive information compromised for each individual (if it varies), the last known mailing address of each individual, and the name and contact information for the vendor's point of contact.
- Require the return or destruction of PHI and other sensitive information after the vendor's work is finished. A BAA must allow a vendor to maintain PHI after the conclusion of the work if it is infeasible to return or destroy the information.<sup>105</sup> The agreement should specify whether the covered entity or business associate decides whether it is feasible. To the extent the vendor receives PHI or other sensitive information that is not necessary for the vendor's work (for example, if the covered entity provides information by mistake), the agreement should require destruction of that information promptly (not at the end of the agreement).
- Require the vendor to cooperate with the entity's investigation of an incident or breach, including providing updates from the vendor's investigation.
- Establish the right to audit the vendor's privacy and security practices, either on a regular basis or upon a breach. The vendor

---

104 45 C.F.R. § 164.410(c).

105 *Id.* § 164.504(e)(2)(ii)(J).

should be required to have a WISP and incident response plan. Many organizations have created robust screening requirements to confirm that vendors' security requirements are sufficient.

- Specify and require safeguards relevant to the context. For example, depending on the service, the entity may want 24/7 video surveillance of sensitive areas, specific password requirements, or encryption of portable devices. Entities should consider requiring representations and warranties that the vendor has performed background checks on all personnel who might work with the covered entity's data.
- Include terms regarding liability for the costs of a breach. The agreement should address whether the business associate is responsible for:
  - All of the covered entity's direct costs (e.g., forensic consultant, attorneys, and mailing).
  - The covered entity's indirect costs (employee time in responding to the breach, lost business).
  - The cost of all services offered to individuals, including those that are not legally required.
- Include terms regarding control of the notification process. In general, covered entities will want exclusive control of the content of notices. Business associates will want a voice in the process to prevent the covered entity from shifting blame unfairly and to keep costs down. The contract should establish:
  - Who decides whether to notify individuals, government regulators, the media, and other third parties.
  - Who controls the content of the notices.
  - Who decides which vendors to retain (e.g., forensic consultant, attorneys, mailing, call center, credit monitoring and identity theft protection services).

*list continues*

–Who decides which products and services to offer affected individuals.

- Address indemnification. Will the vendor indemnify the entity for all damages arising from the breach, regardless of fault? Or will indemnity be limited to harm caused by the vendor's acts or omissions, or some fault standard (e.g., negligence, recklessness, intentional misconduct)? Covered entities will want very broad indemnification, while business associates will want to take on the minimum possible responsibility.
- Require the vendor to carry cyber insurance sufficient to cover the vendor's indemnification obligations. Consider including requirements regarding the scope of coverage, including the per-incident and aggregate dollar limits.

### Establish relationships with organizations that share information on cyber threats

Sharing information about cyber threats can help organizations prioritize their security measures and stay on top of the latest trends and risks. Organizations that have multiple locations (such as hospital systems) need processes to make sure that information about cyber incidents and threats is shared among different locations.

One information-sharing group that might be helpful to health care organizations is the National Health Information Sharing and Analysis Center.<sup>106</sup> Its members are “primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities . . . advice and best practices, mitigation strategies and other valuable material.”<sup>107</sup> A 2016 study showed

---

106 National Health Information Sharing and Analysis Center, NAT'L HEALTH-ISAC, [www.nhisac.org/](http://www.nhisac.org/) (last visited Nov. 26, 2016).

107 *Id.*, <https://nhisac.org/about-nhisac/>.

that “participation in threat sharing” reduced the cost of a data breach by \$9 per compromised record.<sup>108</sup>

### Ensure adequate cyber insurance coverage

Every organization that handles PHI or other sensitive personal information should obtain cyber insurance. Cyber policies vary significantly in terms of the types of incidents they cover, their exclusions, and the coverage amounts. When seeking cyber coverage, organizations should work with a knowledgeable insurance broker or experienced attorney. This is an area where both the law and current risks change quickly, so organizations should review their cyber coverage at least annually.

Legal counsel and other appropriate organizational representatives (such as risk management and members of the incident response team) should review the cyber policy before a security incident or breach. Some insurance policies require organizations to follow minimum security standards, and the organization will need to know the policy’s requirements for giving notice and cooperating with the insurer. Policies might also require the use of pre-approved vendors, such as for legal services, forensic consulting, mailing, and call center staffing.

### Responding to a Breach

The first step in responding to a breach is convening the team that will lead the response. Ideally, this will be the team identified in the [incident response plan](#). If the entity does not have an incident response plan, it should form a committee of high-level personnel with the expertise and authority to command immediate action.

The response team should assign one member the responsibility of documenting all steps of the investigation and response, including the dates and times of all significant events, and the identity of every person involved in the process. It is much easier to document actions as they

---

108 2016 COST OF DATA BREACH STUDY, at 14.

happen, rather than trying to reconstruct them months or years later for a government investigation or litigation. The documentation should stick to verifiable facts and avoid speculation or opinion.

### Address attorney-client privilege and work product protection

An incident investigation might reveal information that could be harmful to the entity if it were disclosed publicly, such as technical vulnerabilities in the entity's computer systems. Many entities therefore choose to have attorneys direct the incident response to protect as much information as possible under the attorney-client privilege and work product doctrine.

If attorneys will direct the incident response, they should retain any forensic investigators directly. The retention agreement should note that the attorneys are engaging the forensic investigators for the purpose of facilitating legal advice to the client (the covered entity or business associate). An attorney should be involved in all communications between the forensic investigators and the client. The forensic investigators should provide drafts of their report to the attorneys for review and approval. As part of that process, counsel should make sure that the report is complete and accurate and does not contain inaccurate information, speculation, or irrelevant details that might be harmful to the client if the report were disclosed to a third party, such as in a government investigation or litigation.

### Instruct personnel to keep information about the breach confidential

The incident response team should strive to keep information about the breach from becoming public until the organization has decided to report it. To minimize the spread of information, the response team should specifically direct every employee who has information about the breach to keep it confidential and not discuss it with anyone unless authorized by the appropriate authority from the response team or management.

### Retain a computer forensic consultant

A forensic consultant can, among other things, help stop an ongoing attack, identify compromised data and systems, and delete malware and other hacker tools from the system. Critically, a qualified forensic expert can preserve digital evidence in case it is needed for a criminal case, civil litigation, or government investigation. If legal counsel is directing the investigation, counsel should retain the forensic consultant so that the consultant's report is privileged.

### Preserve evidence

The entity must retain all information potentially relevant to government investigations or litigation arising from the breach. Depending on the type of breach, the entity might need to make forensic copies of all affected devices and systems, obtain and store electronic logs, preserve video camera footage, or save emails or other communications. The forensic consultant should lead this process and make sure all relevant digital evidence is preserved. The organization's personnel should not try to conduct any electronic investigation except under the supervision and direction of the forensic consultant (or other qualified IT personnel) to avoid destroying evidence inadvertently.

Depending on the size and nature of the breach, the organization might also need to—under the guidance of legal counsel—issue a document-preservation notice to prevent the organization's employees from destroying potentially relevant materials.

### Control the damage

The entity should take whatever steps are necessary to stop the incident (if it is ongoing) and prevent or at least minimize additional harm. That might involve removing affected devices from the network, shutting off unauthorized access to the system, placing physical security devices such as locks on sensitive areas, or suspending or terminating an employee



suspected of participating in a breach. Any actions involving computer systems should be done at the direction, and under the supervision, of a highly qualified technical expert. Organizations should consider whether they have the in-house IT expertise necessary to respond to a security event. For smaller or less technically savvy organizations, it often makes sense to engage an outside breach-management vendor.

### Decide whether to contact law enforcement

A health care organization must balance the potential benefits of contacting law enforcement with the risk of losing control over the investigation. For most breaches, there is no reason to report to law enforcement. Getting law enforcement involved makes sense, however, when the person or people responsible for the breach should be held accountable, or where the government's powers of investigation (such as the ability to obtain subpoenas and search warrants) would be helpful. Another reason to contact law enforcement is to try to get a request to delay notifications, as explained [earlier](#).

Incidents that involve the exfiltration (removal) of data from a computer system can be reported to either the FBI's cybercrimes unit or to the U.S. Secret Service. Breaches that involve paper records or known perpetrators (such as employees) can be reported to the local police department.

The cybersecurity unit of the U.S. Department of Justice (DOJ) also recommends that organizations consider contacting the National Cybersecurity & Communications Integration Center (NCCIC), which is available 24/7. According to the DOJ's cybersecurity unit, "By contacting the NCCIC, a victim organization can both share and receive information about an ongoing incident that may prove beneficial to both the victim organization and the government. A victim organization may also obtain technical assistance capable of mitigating an ongoing cyber incident."<sup>109</sup>

---

109 BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS, at 11–12.

### Interview personnel

Members of the incident response team should document key facts and interview everyone who has information about the incident as soon as possible, before memories fade and key documents are lost. If the investigation is being led by counsel, an attorney should participate in the interviews and in drafting written summaries of them. To maximize the chances of protection under the work product doctrine, written summaries should include the observations, opinions, and thoughts of the attorney, as opposed to verbatim transcripts of the witnesses' statements.<sup>110</sup>

### Notify insurance carriers

The entity should immediately notify all insurers whose policies might provide coverage for the incident, including cyber insurance, commercial general liability, professional liability, errors and omissions, and other types of policies. Insurance policies generally require prompt notice and cooperation with the insurer's protocols and claim investigation.

### Decide whether to report the breach

The entity must determine whether it has a legal obligation to report under [HIPAA](#) and [state laws](#). It should also determine whether it has contractual obligations to report the breach under BAAs or other contracts.

### Prepare for communications with media and other third parties

In addition to drafting any media notice required by HIPAA or other law, the organization should proactively prepare to respond to questions about the breach from the media and other third parties, such

---

110 See *Upjohn Co. v. United States*, 449 U.S. 383, 401–02 (1981) (discussing the very significant showing of necessity that is required for disclosure of materials that reveals an attorney's mental processes); FED. R. CIV. P. 26(b)(3)(B).

as patients, customers, and business partners. Depending on the size and nature of the breach, the organization should consider retaining a public relations firm that has experience dealing with data breaches. The firm may have personal contacts within the media, which could help de-sensationalize reporting. A public relations firm will also be trained in clear, concise communication and can help avoid “legalese” in the notices.

### Draft notices

Legal counsel should participate in the drafting to make sure notices comply with all legal requirements and minimize the possibility that the notices might harm the organization during a later government investigation or litigation. An employee or outside consultant with experience in communications or public relations should also participate, if possible. The notices should be approved by the appropriate representative(s) of the organization (who ideally will be specified in the incident response plan and/or breach reporting policy).

### Decide what services to offer affected individuals

There is generally no legal requirement to provide credit monitoring or identity theft protection services, although California requires any entity that chooses to provide identity theft protection and mitigation services to provide them for at least 12 months.<sup>111</sup> Entities generally offer these services to individuals for 1–3 years,<sup>112</sup> and should carefully screen the vendors that provide these services. In previous breaches, vendors

---

<sup>111</sup> CAL. CIV. CODE § 1798.82(d)(2).

<sup>112</sup> See DEP'T OF THE NAVY, FREQUENTLY ASKED QUESTIONS: OPM DATA BREACH 4 (2015), available at [www.secnav.navy.mil/OPMBreachDON/Documents/2015/09/DON\\_OPM\\_Breach\\_FAQs\\_091515.pdf](http://www.secnav.navy.mil/OPMBreachDON/Documents/2015/09/DON_OPM_Breach_FAQs_091515.pdf) (noting that the federal government had offered either 18 months or 3 years of ID theft protection services to people affected by two different incidents); Michael Hiltzik, *Anthem is Warning Consumers About its Huge Data Breach. Here's a Translation.*, L.A. TIMES (Mar. 6, 2015, 10:34 AM), [www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html](http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html) (noting that Anthem offered 2 years of ID theft protection).

have been criticized for providing false or misleading information to consumers, or for trying to upsell more expensive services to affected individuals. Entities must also assess what information the vendor will need to implement the services offered (i.e., whether the vendor needs individuals' information in advance to issue registration codes).

### Make logistical arrangements

For breaches of any significant size, the logistics of notifications can require a significant amount of time and resources. It is important to start thinking about them early in the process. Depending on what notifications and services the organization has decided to provide, it needs to make arrangements for either its personnel or outside vendors to:

- Compile a spreadsheet of all the names, addresses, and types of PHI compromised for all affected individuals (making sure to remove duplicate names). For very large breaches, the entity might have to hire outside consulting help to assist in understanding which individuals have been affected and de-duplicating the contact information.
- Prepare, print, and mail letters for individual notices. It takes a substantial amount of time to print and stuff envelopes for breaches involving hundreds of thousands or millions of individuals.
- Run all individuals' addresses through the U.S. Postal Service's change-of-address database. That will reduce the amount of returned mail and might allow the entity to send the letters first class (as required by HIPAA) but at the bulk mail rate.
- Determine who will handle calls from individuals who have questions or want to activate any offered credit monitoring or identity theft services. For significant breaches, this is usu-

ally outsourced to a call center. We recommend that the entity provide a script to the call center with responses to FAQs and a process for escalating calls to a representative of the breached entity. The entity should closely examine whether the call center has the capacity to handle the anticipated call volume, including its back-up procedures in case call volume is greater than expected.

### Document all steps of the breach response

Proper documentation is required by HIPAA and is a best practice for all types of breaches. Under HIPAA, a covered entity or business associate must maintain documentation demonstrating either that the organization made all required notifications or that notification was not required.<sup>113</sup> HIPAA also requires covered entities and business associates to develop and document policies and procedures governing breach incidents and to retain in writing, for a period of six years, policies and procedures and any other activity (e.g., employee sanctions) that must be documented.<sup>114</sup>

### Adopt and implement a corrective action plan

After an organization determines that an incident is a reportable breach, the organization should focus on mitigation and documenting a corrective action plan. Key areas to focus on when taking corrective action are:

- Mitigating the risk to individuals affected by the breach.
- Addressing the systemic problems that created the breach. For example, if the breach involved the loss of an unencrypted

---

<sup>113</sup> 45 C.F.R. § 164.414(b); 78 Fed. Reg. 5566, 5657–58.

<sup>114</sup> 45 C.F.R. § 164.414(a); 78 Fed. Reg. at 5657.

laptop, the organization should implement a program for encrypting all laptops and other portable media.

- Implementing appropriate discipline for the personnel who caused the breach (consistent with the organization's personnel policies).
- Providing additional training. This should include training on any systemic fixes to address the breach, policy changes, and other information that will be relevant to the organization's personnel.

Organizations should start corrective actions as soon as possible. HIPAA provides an affirmative defense to civil money penalties for breaches that were not due to willful misconduct and are corrected during "[t]he 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred . . . ."<sup>115</sup> All corrective actions should be documented, and the organization should retain such documentation for at least six years.<sup>116</sup>

### Perform or update the security risk analysis

After a breach, organizations should update their security risk analysis and risk management plan. If an organization has not undergone a security risk analysis, it should perform one right away and start implementing a risk management plan. In the authors' experience, OCR investigators routinely ask for a copy of the organization's risk analysis at the beginning of an investigation.

---

<sup>115</sup> 45 C.F.R. § 160.410(c)(2)(i).

<sup>116</sup> *Id.* § 164.316(b).

## Conclusion

Data breaches are now a reality of doing business, particularly for health care organizations. Appropriate prevention can reduce the likelihood of a breach, and preparation can reduce the associated costs. However, the health care industry and its regulators should take a long and hard look at whether the present breach-reporting requirements should be changed. Dealing with a large data breach is incredibly expensive, especially for many community hospitals and physician groups that operate on a thin profit margin. It is debatable whether notice to individuals makes a difference in the majority of instances where reporting is required. People are weary of data breaches and often do not bother to sign up for any offered credit monitoring or identity theft resolution services.

Perhaps a wiser path would be to institute individual authentication requirements for obtaining credit and other services, so that identity thieves could not use the breached data for those purposes. Another option would be for CMS and other payers to institute smarter algorithms to catch fraudulent claims. Ultimately, what would help consumers most is a system that requires reporting to individuals who must know about the breach in order to protect themselves. Modifying the reporting requirements to provide real protection to individuals in a manner that is less financially burdensome to the health care industry would benefit everyone.



**American Health Lawyers Association**

1620 Eye Street, NW, 6th Floor • Washington, DC 20006-4010  
(202) 833-1100 • Fax (202) 833-1105 • [www.healthlawyers.org](http://www.healthlawyers.org)